Avira AntiVir WebGate / Avira WebGate Suite

Handbuch für Anwender

AVIRA

Inhalt

1 Über dieses Handbuch

Dieses Kapitel enthält einen Überblick über den Aufbau und den Inhalt dieses Handbuchs.

Auf eine kurze Einleitung folgen Informationen zu den folgenden Themen:

Aufbau des Handbuchs

Zeichen und Symbole

Abkürzungen

1.1 Einleitung

In diesem Handbuch haben wir für Sie alle nötigen Informationen über Avira AntiVir WebGate zusammengestellt und führen Sie Schritt für Schritt durch die Installation, Konfiguration und Bedienung der Software.

Im Anhang finden Sie ein Glossar, in dem grundlegende Begriffe erläutert werden.

Die im Produktpaket enthaltene Datei RELEASE_INFOS enthält weitere aktuelle Informationen über Avira AntiVir WebGate.

Weitere Informationen und Hilfestellungen bieten Ihnen darüber hinaus unsere Webseite, die Hotline unseres Technischen Supports und unser regelmäßiger Newsletter .

Ihr Avira-Team

1.2 Aufbau des Handbuchs

Das Handbuch zu Ihrer AntiVir-Software besteht aus mehreren Kapiteln, in denen Sie folgende Informationen finden:

Kapitel	**Inhalt**
Über dieses Handbuch	Aufbau des Handbuchs, Zeichen und Symbole.
Produktinformationen	Allgemeine Hinweise zu Avira AntiVir WebGate, den Modulen, Leistungsmerkmalen und Systemanforderungen sowie zur Lizenzierung.
Installation	Eine Anleitung zur Installation von Avira AntiVir WebGate auf Ihrem System.
Konfiguration	Hinweise zur optimalen Einstellung von Avira AntiVir WebGate auf Ihrem System.
Betrieb	Arbeiten mit Avira AntiVir WebGate und Verhalten bei der Erkennung von Viren und unerwünschten Programmen.
Aktualisierungen	Ausführen manueller oder automatischer Aktualisierungen.
Service	Avira Operations GmbH & Co. KG Support und Service.
Anhang	Glossar mit Erläuterungen von Fachbegriffen und Abkürzungen. Goldene Regeln zum Schutz vor Viren.

1.3

Hervorhebung im Text	**Erläuterung**
Strg+Alt	Tasten oder Tastenkombinationen
/usr/lib/AntiVir/webgate/avupdate-webgate	Pfadangaben und Dateinamen
`ls /usr/lib/AntiVir/webgate`	Benutzereingaben
Komponente auswählen **Alles auswählen**	Elemente der Software-Oberfläche, z. B. Menüoptionen, Fenstertitel oder Schaltflächen in Dialogfenstern
http://www.avira.com	URLs
– Page 5	Querverweise innerhalb des Dokuments

1.4 Abkürzungen

In diesem Handbuch werden die folgenden Abkürzungen verwendet:

Abkürzung	Bedeutung
ACL	Access Control List
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICAP	Internet Content Adaptation Protocol
SMTP	Simple Mail Transfer Protocol
SNEWS	Secure News Server
SSL	Secure Sockets Layer
VDF	Virus Definition File

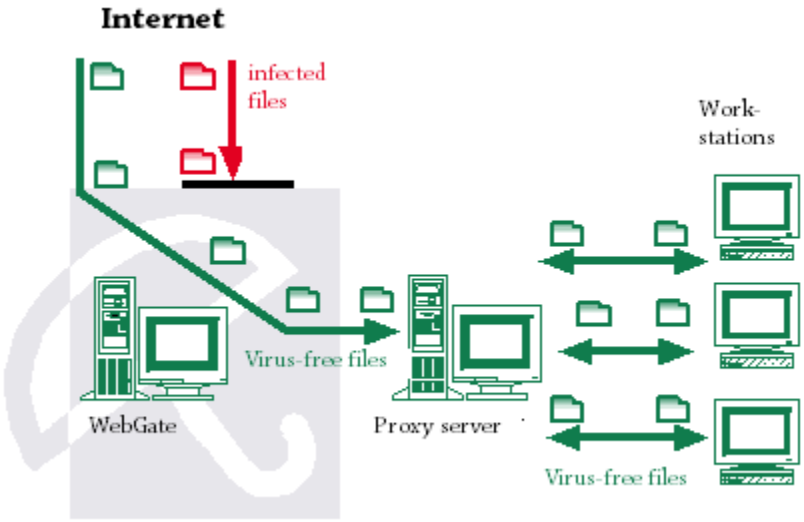
2 Produktinformationen

Die Verbindung eines Computers zum Internet wird als Eintrittspforte für Malware immer noch unterschätzt. Wenn Sie ungefilterte Daten aus dem Internet auf Ihr System übertragen, können sich alle Arten von Malware im gesamten Netzwerk verbreiten.

Avira AntiVir WebGate prüft und filtert alle Dateien aus dem Internet, blockiert bei Bedarf den Zugriff darauf und stellt so einen zuverlässigen Schutz für Ihren Computer dar.

Außerdem prüft Avira AntiVir WebGate den gesamten ausgehenden Datenverkehr.

Firmencomputer greifen normalerweise über einen Proxyserver – d. h. indirekt – auf das Internet zu. Avira AntiVir WebGate arbeitet mit dem Proxyserver zusammen und ergänzt ihn auf ideale Weise.Zunächst zwei sehr wichtige



Hinweise:

Warnung: *Der Verlust wertvoller Daten hat meist dramatische Folgen. Auch die beste Antivirensoftware kann Sie nicht hundertprozentig vor Datenverlust schützen.*

Legen Sie regelmäßig Sicherungskopien Ihrer Dateien an.

Warnung: *Ein Antivirenprogramm ist nur dann zuverlässig und wirksam, wenn es aktuell ist.*

Stellen Sie durch automatische Aktualisierungen sicher, dass Ihr Avira AntiVir WebGate stets auf dem neuesten Stand ist. In diesem Handbuch erfahren Sie, wie Sie dabei vorgehen.

2.1 Leistungsmerkmale

Avira AntiVir WebGate unterstützt eine Vielzahl von Konfigurationseinstellungen, mit denen die Datenübertragung im Internet überwacht werden kann. Die wichtigsten Leistungsmerkmale:

- Mit der erweiterten Zugriffssteuerung können Regeln aufgestellt werden, die ein Tunneln bestimmter Anfrage- und Antworttypen ermöglichen.
- Lokale URL-Filterung unter Verwendung der Kategorien in der Avira-URL-Filterbibliothek
- Online-URL-Filterung unter Verwendung der Kategorien in der Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung (verfügbar in **Avira WebGate Suite**)
- Echtzeitprüfung auf Viren und unerwünschte Programme
- Heuristische Erkennung von Makroviren
- Prüfung aller heruntergeladenen Dateien (HTTP und FTP)
- Prüfung aller ausgehenden Dateien (z. B. PUT und POST)
- Erkennung aller gebräuchlichen Archivtypen
- Automatische Internet-Aktualisierung des Produkts, der Scan-Engine und der VDF
- Konfigurierbare Benachrichtigungsfunktionen für den Administrator (Protokolle, Warnungen und Berichte) und Versenden von Email-Warnungen (SMTP)
- Selbst-Integritätsprüfung des Programms, um sicherzustellen, dass das Antivirensystem korrekt arbeitet
- Steuerung des Zugriffs auf WebGate mithilfe von IP-Adressen
- ICAP-Unterstützung (ermöglicht Verbindung über ICAP-Schnittstelle)

2.2 Lizenzierungskonzept

Um Avira AntiVir WebGate nutzen zu können, benötigen Sie eine Lizenz.
Die Lizenzbedingungen müssen akzeptiert werden
(siehe http://www.avira.com/de/license-agreement).

Für Avira AntiVir WebGate gibt es zwei Lizenzmodelle:

- Testversion
- Vollversion

Die Lizenz hängt von der Anzahl der Benutzer im Netzwerk ab, die durch Avira AntiVir WebGate geschützt werden sollen.

Die Lizenz wird über eine Lizenzdatei namens hbedv.key vergeben. Sie erhalten diese Datei per Email von der Avira Operations GmbH & Co. KG. Die Datei enthält genaue Angaben darüber, welche Programme für welchen Zeitraum lizenziert sind. Eine Lizenzdatei kann für mehrere Avira-Produkte gelten.

Testversion

Weitere Informationen zur 30-Tage-Testlizenz finden Sie auf unserer Website:

http://www.avira.com/de.

Vollversion

Zum Leistungsumfang der Vollversion gehören:

- Herunterladen der Avira AntiVir WebGate-Versionen aus dem Internet

- Lizenzdatei per Email zum Freischalten der Testversion zur Vollversion
- Ausführliche Installationsanleitung (digital)
- Vierwöchiger Installationssupport ab Kaufdatum
- Newsletter-Dienst (per Email)
- Internet-Update-Service für Programmdateien und VDF

Nach der Installation eines AntiVir-Produkts können Sie sich mit dem Lizenz-Tool avlinfo Informationen über die aktuelle Lizenz anzeigen lassen:

Wechseln Sie in das Verzeichnis /usr/lib/AntiVir/webgate, und rufen Sie `./avlinfo` auf.

Mit `avlinfo -h` erhalten Sie Informationen über die Verwendung des Tools.

2.3 Module und Funktionsweise von Avira AntiVir WebGate

Die Avira AntiVir WebGate-Sicherheitssoftware setzt sich aus folgenden Modulen zusammen:

- AntiVir Engine
- Avira Updater
- WebGate-Hauptprogramm
- Avira-URL-Filterbibliothek
- Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung

AntiVir Engine

AntiVir Engine besteht hauptsächlich aus den Prüf- und Reparaturmodulen der Avira-Software.

Avira Updater

Avira Updater lädt in regelmäßigen Zeitabständen die neuesten Aktualisierungen von den Avira AntiVir-Webservern herunter und installiert sie (manuell oder automatisch). Das Modul kann auch Benachrichtigungen per Email versenden.

Sie können Avira AntiVir WebGate insgesamt oder komponentenweise aktualisieren, also z. B. nur die Signaturen, das Avira Engine-Modul oder den Scanner.

WebGate-Hauptprogramm

Das Hauptprogramm enthält die eigentlichen WebGate-Funktionen. Es überwacht den HTTP- und FTP-Netzwerkzugriff über das Internet. Mithilfe von Avira AntiVir Engine werden Viren und unerwünschte Programme erkannt.

Avira-URL-Filterbibliothek

Avira AntiVir WebGate stellt durch einen lokalen Filter anhand einer Liste bekannter URLs fest, ob eine URL gefährlich ist. Die URLs in der Liste sind in drei

Gruppen unterteilt: Malware, Phishing und Betrug. Aus Sicherheitsgründen ist der Avira-URL-Filter in jeder gültigen WebGate- oder WebGate Suite-Installation aktiviert.

Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung

AntiVir WebGate erlaubt Clients, ausgehende Anforderungen anhand von URL-Kategorien zu filtern (z. B. *Gewalt*, *Glücksspiel*, *Pornographie* usw.). Die Kategorien einer bestimmten URL werden anhand der Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung ermittelt. (Dieses Modul wird nur mit der Lizenz für **Avira WebGate Suite** aktiviert.)

Weitere Informationen zur Bibliothek für die Webzugriffs- und Inhaltssteuerung finden Sie im WebGate-Installationsverzeichnis.

2.3.1 Systemanforderungen

Ein System, auf dem Avira AntiVir WebGate laufen soll, muss die folgenden Mindestanforderungen erfüllen:

- Computer: x386, Sparc
- BS: Linux oder Sun Solaris
- CPU: 32-Bit- oder 64-Bit-UNIX
  Die Ausführung der AntiVir-Software auf Systemen mit 64-Bit-UNIX setzt voraus, dass 32-Bit-Binärdateien ausgeführt werden können. Eine Anleitung dazu, wie Sie dieses Verhalten überprüfen und ggf. aktivieren können, finden Sie in der Dokumentation Ihres UNIX-Systems.
- HD: 100 MB (1 GB oder mehr empfohlen)
- RAM: 256 MB (1280 MB für Solaris)

Die Versionen für Linux und Solaris verwenden ähnliche Installations- und Betriebsverfahren (im Normalfall unterscheiden sich je nach Zielsystem nur einige Dateinamen).

Offiziell unterstützte Distributionen für Avira AntiVir WebGate und Avira WebGate Suite:

- Red Hat Enterprise Linux (RHEL) Server 5.8
- Red Hat Enterprise Linux (RHEL) Server 6.2
- Novell SUSE Linux Enterprise Server (SLES) 11 SP2
- Novell SUSE Linux Enterprise Server (SLES) 10 SP4
- Debian GNU/Linux 5.0
- Debian GNU/Linux 6.0
- Ubuntu Server 10.04 LTS
- Ubuntu Server 11.10
- Ubuntu Server 12.04 LTS
- Sun Solaris 9 (SPARC)*
- Sun Solaris 10 (SPARC)

* wird unterstützt bis 31.12.2012

3 Installation

Die aktuelle Version von Avira AntiVir WebGate finden Sie auf unserer Website: http://www.avira.com/de/support-download-avira-antivir-webgate.

Avira AntiVir WebGate wird als komprimiertes Archiv zur Verfügung gestellt. Dieses Archiv enthält AntiVir Engine, die VDF-Dateien, Avira Updater, das WebGate-Hauptprogramm und das optionale SMC-Plugin.

Sie werden Schritt für Schritt durch die Installation geführt. Dieses Kapitel besteht aus folgenden Abschnitten:

Auswahl des WebGate-Computers

Installationsdateien bereitstellen

Lizenzierung

Avira AntiVir WebGate installieren

AntiVir erneut installieren und deinstallieren

3.1 Auswahl des WebGate-Computers

Je nach Netzwerk- und Hardwarekonfiguration gibt es verschiedene Möglichkeiten, einen Computer mit Avira AntiVir WebGate als „Wächter“ zwischen dem Client des Benutzers und dem Internet zu platzieren.

Um einen geregelten Internetzugang sicherzustellen, wird eine Verbindung zum Proxyserver benötigt.

Avira AntiVir WebGate wird zuerst an die Netzwerkkonfiguration angepasst . Während der Installation muss entschieden werden, auf welchem Computer WebGate installiert wird.

Achtung: Wenn Sie auch Avira AntiVir UNIX Server oder Avira AntiVir Professional (UNIX) installiert haben und diese Produkte mithilfe der GUI konfigurieren und betreiben, beachten Sie, dass die GUI mit den aktuellen Versionen (beginnend mit Version 3) von Avira AntiVir UNIX MailGate und Avira AntiVir UNIX WebGate nicht kompatibel ist.

3.2 Installationsdateien bereitstellen

Installationsdateien aus dem Internet herunterladen

Laden Sie die Dateien der aktuellen Version von unserer Website http://www.avira.com/de/support-download-avira-antivir-webgate auf Ihren lokalen Computer herunter. Der Dateiname lautet antivir-webgate-prof.tar.gz.

Speichern Sie die Datei in einem */tmp*-Ordner auf dem Computer, auf dem WebGate laufen soll.

Programmdateien entpacken

Wechseln Sie in das temporäre Verzeichnis:

```
cd /tmp
```

Entpacken Sie das Avira AntiVir WebGate Archiv:

```
tar -xzvf antivir-webgate-prof-<Version>.tar.gz
```

Im temporären Verzeichnis finden Sie nun antivir-webgate-prof-<Version>.

3.3 Lizenzierung

Um AntiVir WebGate verwenden zu können, benötigen Sie eine Lizenz (siehe Lizenzierungskonzept). Die Lizenz wird in einer Datei namens hbedv.key bereitgestellt.

Diese Lizenzdatei enthält Informationen über den Umfang und die Gültigkeitsdauer der Lizenz.

Lizenz erwerben

Auf unserer Website (http://www.avira.com) können Sie eine 30-Tage-Testlizenz für Avira AntiVir WebGate anfordern.

Die Lizenzdatei wird Ihnen per Email zugesandt.

Sie können Avira AntiVir WebGate auch einfach in unserem Online-Shop erwerben (Details dazu finden Sie unter http://www.avira.com).

Lizenzdatei kopieren

Kopieren Sie die Lizenzdatei hbedv.key in das Installationsverzeichnis auf Ihrem System: /tmp/antivir-webgate-prof-<Version>.

3.4 Avira AntiVir WebGate installieren

Die Installation von Avira AntiVir WebGate erfolgt automatisch über ein Installationsskript. Dieses Skript führt folgende Aufgaben aus:

- Prüfen der Integrität der Installationsdateien
- Prüfen der für die Installation erforderlichen Berechtigungen
- Suchen nach auf dem Computer bereits installierten Versionen von AntiVir-Produkten
- Kopieren der Programmdateien und Überschreiben vorhandener Dateien, die nicht mehr benötigt werden
- Kopieren der Konfigurationsdateien, wobei vorhandene AntiVir-Konfigurationsdateien erhalten bleiben
- Installieren von Avira Updater
- Optional: Installieren des Plugins für SMC
- Optional: Konfigurieren der automatischen Startfunktion von Avira AntiVir WebGate und des Avira Updaters

Bei der ersten Installation müssen Sie die folgenden Schritte durchführen:

Installation vorbereiten

Melden Sie sich als **root** an. Andernfalls reicht Ihre Berechtigung nicht aus, um die Installation durchzuführen, und das Skript gibt eine Fehlermeldung aus.

Achtung: Um Avira Antivir WebGate auf einem Client mit aktiver Firewall auszuführen, benötigt WebGate die folgenden geöffneten Ports: `localhost tcp: 50358` (nur für SMC-Benutzer) und `udp port 51973` (wenn `DBSupport` auf `YES` gesetzt ist)

Wechseln Sie in das Verzeichnis, in dem Sie Avira AntiVir WebGate entpackt haben:

```
cd /tmp/antivir-webgate-prof-<Version>
```

Avira AntiVir WebGate installieren

Hinweis: Das genaue Installationsverfahren hängt davon ab, welche AntiVir-Produkte bereits auf Ihrem Computer installiert sind.

Geben Sie Folgendes ein:

```
./install
```

Bestätigen Sie die Lizenzvereinbarung.

Das Installationsskript wird gestartet. Zuerst werden die AntiVir-Grundkomponenten installiert:

```
Do you agree to the license terms? [n] y

creating /usr/lib/AntiVir/webgate ... done
copying LICENSE to /usr/lib/AntiVir/webgate/LICENSE-webgate ... done
1) installing AntiVir Core Components (Engine, Savapi and Avupdate)
copying uninstall to /usr/lib/AntiVir/webgate... done
copying uninstall_smcplugin.sh to /usr/lib/AntiVir/webgate ... done
```

Nachdem Sie den Pfad der Schlüsseldatei eingegeben haben, fährt das Installationsprogramm mit der Konfiguration der Aktualisierungen fort:

```
Enter the path to your key file: [] /root/Desktop/HBEDV.KEY
copying /root/Desktop/HBEDV.KEY to /usr/lib/AntiVir/webgate/hbedv.key ...
done
installation of AntiVir Core Components (Engine, Savapi and Avupdate) com-
plete

2) Configuring updates
An internet updater is available...
...

Would you like to create a link in /usr/sbin for avupdate-webgate ? [y]
```

Geben Sie **Y** ein.

Danach kann das Skript einen cron-Task für automatische Scanner-Updates erstellen:

```
linking /usr/sbin/avupdate-webgate to /usr/lib/AntiVir/webgate/avupdate-webgate ... done

Would you like to setup Scanner update as cron task ? [y]
```

Geben Sie **Y** ein, wenn diese cron-Tasks erstellt werden sollen.

Legen Sie nun das Intervall fest, in dem nach Aktualisierungen gesucht werden soll:

```
Please specify the interval to check.
Recommended values are daily or 2 hours.

available options: d [2]
```

Drücken Sie die **Eingabetaste**, wenn alle zwei Stunden nach Aktualisierungen gesucht werden soll. Für eine tägliche Suche geben Sie **d** ein.

Nun möchte das Skript wissen, ob einmal pro Woche nach Produktaktualisierungen gesucht werden soll:

```
creating Scanner update cronjob ... done

Would you like to check for WebGate updates once a week ? [n]
```

Geben Sie **Y** ein, wenn dieser Task erstellt werden soll.

Der nächste Schritt ist die Installation des Hauptprogramms:

```
creating WebGate update cronjob ... done

setup internet updater complete

3) installing main program
copying doc/antivir_webgate_en.pdf to /usr/lib/AntiVir/webgate ... done
copying bin/linux_glibc22/avwebgate.bin to /usr/lib/AntiVir/webgate... done
```

Das Programm wird installiert. Nun werden Sie gefragt, ob Sie einen Link auf avwebgate erstellen möchten und ob der Updater beim Systemstart automatisch gestartet werden soll:

```
Would you like to create a link in /usr/sbin for avwebgate ? [y]
linking /usr/sbin/avwebgate to /usr/lib/AntiVir/webgate/avwebgate ... done

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

Bestätigen Sie durch Drücken der **Eingabetaste**. Sie können diese Einstellungen später ändern.

Der automatische Systemstart wird konfiguriert:

```
setting up boot script ... done
installation of main program complete
```

Nun werden Sie gefragt, ob Sie WebGate mit dem optionalen Plugin für AntiVir Security Management Center installieren möchten.

```
4) activate SMC support
If you are going to use AVIRA Security Management Center (SMC)
to manage this software remotely you need this

Would you like to activate SMC support? [y]
```

Wenn Sie Avira SMC verwenden:

Geben Sie **Y** ein, oder bestätigen Sie mit der **Eingabetaste**.

Das Plugin wird installiert und die Installation abgeschlossen:

```
Installation of the following features complete:
  AntiVir Core Components (Engine, Savapi and Avupdate)
  AVIRA Internet Updater
  AVIRA WebGate
  AntiVir SMC plugin
```

Nun können Sie Avira AntiVir WebGate starten:

```
/usr/lib/AntiVir/webgate/avwebgate start
```

Geänderte Binärdateien sind nicht lauffähig.
Wenn Binärdateien z. B. vor der Ausführung verlinkt werden: Deaktivieren Sie die Prelink-Funktion, oder fügen Sie /usr/lib/AntiVir/webgate als ausgeschlossenen Prelink-Pfad in /etc/prelink.conf ein.

***Warnung**: Seit der Version 3.0.0 wird ein neues Scanner-Backend verwendet. Ältere scannerspezifische Konfigurationsoptionen, die WebGate nicht erkennt, müssen aus der Datei*
/etc/avira/avwebgate.conf
in die folgende scannerspezifische Konfigurationsdatei verlegt werden:
/etc/avira/avwebgate-scanner.conf.

***Achtung:** Es empfiehlt sich dringend, nach der Installation eine Aktualisierung durchzuführen, damit alle Schutzmechanismen auf dem neuesten Stand sind. Führen Sie dazu den folgenden Befehl aus:*

```
/usr/lib/AntiVir/webgate/avupdate-webgate
--product=WebGate
```

Weitere Informationen über Aktualisierungen finden Sie unter Aktualisierungen – Seite 90.

3.5 AntiVir erneut installieren und deinstallieren

Sie können das Installationsskript jederzeit nochmals ausführen. Dies ist z. B. in folgenden Situationen sinnvoll:

- Installation einer neuen Version (Upgrade). Das Installationsskript prüft die Vorgängerversion und installiert die erforderlichen neuen Komponenten. Die vorhandenen Konfigurationseinstellungen werden dabei nicht überschrieben, sondern beibehalten .
- Spätere Installation bestimmter Komponenten.
- Aktivieren oder Deaktivieren der automatischen Startfunktion von Avira AntiVir WebGate oder des Avira Updaters.

Avira AntiVir WebGate erneut installieren

Das Verfahren ist für alle obigen Fälle dasselbe:

Wechseln Sie in das temporäre Verzeichnis, in dem Sie Avira AntiVir WebGate entpackt haben:

```
cd /tmp/antivir-webgate-prof-<Version>
```

Geben Sie Folgendes ein:

```
./install
```

Das Installationsskript wird wie oben beschrieben ausgeführt (siehe Avira AntiVir WebGate installieren).

Nehmen Sie während der Installation die erforderlichen Änderungen vor.

Avira AntiVir WebGate wird mit den gewünschten Einstellungen installiert.

AntiVir deinstallieren

Wenn Sie Avira Antivir WebGate deinstallieren möchten, können Sie das Skript *uninstall* verwenden, das in Ihrem Installationverzeichnis liegt. Die Syntax lautet:

```
uninstall [--product=Produktname] [--no-interactive]
[--inf=inf file] [--force] [--skip] [--version] [--help]
```

Der `Produktname` ist `Webgate.`

Öffnen Sie das Verzeichnis, in das Sie Avira AntiVir WebGate installiert haben:

```
cd /usr/lib/AntiVir/webgate
```

Geben Sie Folgendes ein:

```
./uninstall --product=Webgate
```

Das Skript beginnt mit der Deinstallation des Produkts. Sie werden gefragt, ob Sie Sicherungskopien der Lizenzdatei, der Konfigurationsdateien und der Logdateien anlegen möchten. Auch die cron-Tasks für WebGate und den Scanner werden auf Wunsch entfernt.

Beantworten Sie die entsprechenden Fragen mit **y** oder **n**, und drücken Sie die **Eingabetaste**.

AntiVir WebGate wird von Ihrem System gelöscht.

4 Konfiguration

Avira AntiVir WebGate kann so konfiguriert werden, dass immer die optimale Leistung erreicht wird. Die Vorschläge in diesem Kapitel stellen die gebräuchlichsten Einstellungen dar. Sie können diese Einstellungen jederzeit ändern, um WebGate an Ihre Anforderungen anzupassen.

Sie werden Schritt für Schritt durch den Konfigurationsvorgang geführt:

- Im Abschnitt HTTP-Verkehr überwachen – Seite 18 erhalten Sie einen Überblick über die verschiedenen Möglichkeiten, WebGate innerhalb Ihres Netzwerks einzusetzen.
- Unter FTP-Verkehr überwachen – Seite 22 wird beschrieben, wie WebGate als FTP-Proxy eingesetzt werden kann.
- Einbindung über die ICAP-Schnittstelle – Seite 24 enthält Informationen zur Einbindung von WebGate über die ICAP-Schnittstelle.
- Konfigurationsdateien – Seite 26 beschreibt die Parameterwerte für Produkt, Scanner, Updater und ACL.
- Unter Vorlagenkonfiguration – Seite 47 wird erläutert, wie die von WebGate zu Benachrichtigungszwecken erzeugten Webseiten und Emails angepasst werden können.

4.1 HTTP-Verkehr überwachen

WebGate kann den gesamten ein- und ausgehenden HTTP-Datenverkehr nach Viren und unerwünschten Programmen durchsuchen. Auch die über webbasiertes FTP übertragenen Daten können geprüft werden (FTP über HTTP). WebGate arbeitet mit vorhandenen Proxyservern zusammen und ergänzt sie, kann aber auch als eigenständiger HTTP-Proxy eingesetzt werden.

Je nach vorhandener Netzwerk- und Hardwarekonfiguration bieten sich verschiedene Möglichkeiten, Avira AntiVir WebGate als „Wächter“ zwischen Client-Computer und Internet zu platzieren. In allen genannten Fällen greift der Benutzer nicht direkt, sondern über WebGate auf das Internet zu.

Sie können zwischen drei verschiedenen Konfigurationen wählen:

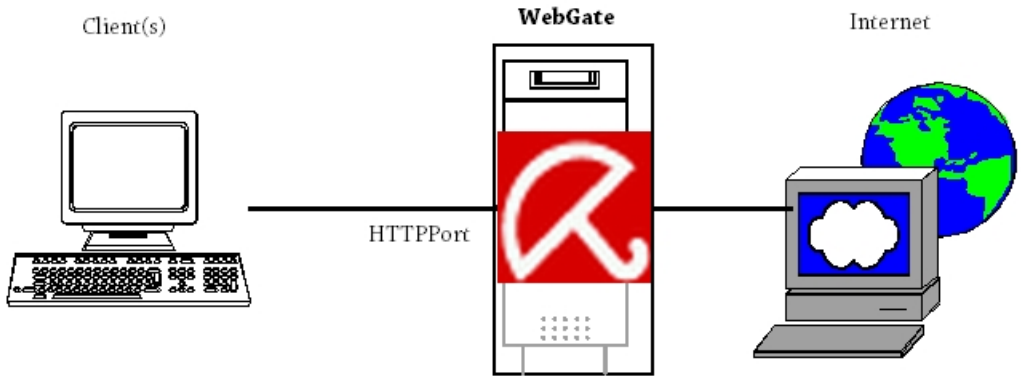
- WebGate ohne Proxyserver (Netzwerkkonfiguration 0) – Seite 19
- WebGate zwischen Client und Proxyserver (Netzwerkkonfiguration 1) – Seite 19
- WebGate zwischen Proxyserver und Internet (Netzwerkkonfiguration 2) – Seite 21

Wenn Sie bei der Konfiguration Ports unter 1024 einstellen, müssen Sie WebGate als root ausführen.

WebGate ohne Proxyserver (Netzwerkkonfiguration 0)

Wenn kein Proxyserver vorhanden ist, operiert WebGate zwischen den Clients und dem Internet. Es kann direkt auf den Clients oder auf einem anderen Computer installiert werden.

WebGate leitet die Anfragen der Clients an das Internet weiter und prüft die Antworten aus dem Internet. Der Zugriff auf infizierte Dateien einer Website wird gesperrt. Nur nicht infizierte Dateien werden an die Clients weitergeleitet. Aus der Sicht eines Clients funktioniert WebGate wie ein Proxyserver.



▶ Nehmen Sie in avwebgate.conf die folgenden Einstellungen vor (Beispiel):

```
HTTPPort 8080
```

▶ Konfigurieren Sie den Browser entsprechend der Clients.

Wenn WebGate auf dem Client selbst installiert ist, empfiehlt sich für avwebgate.conf *die folgende Einstellung:*

```
HTTPPort 127.0.0.1:8080
```

▶ Geben Sie für **HTTP Proxy** die IP-Adresse `127.0.0.1` oder `localhost` ein.

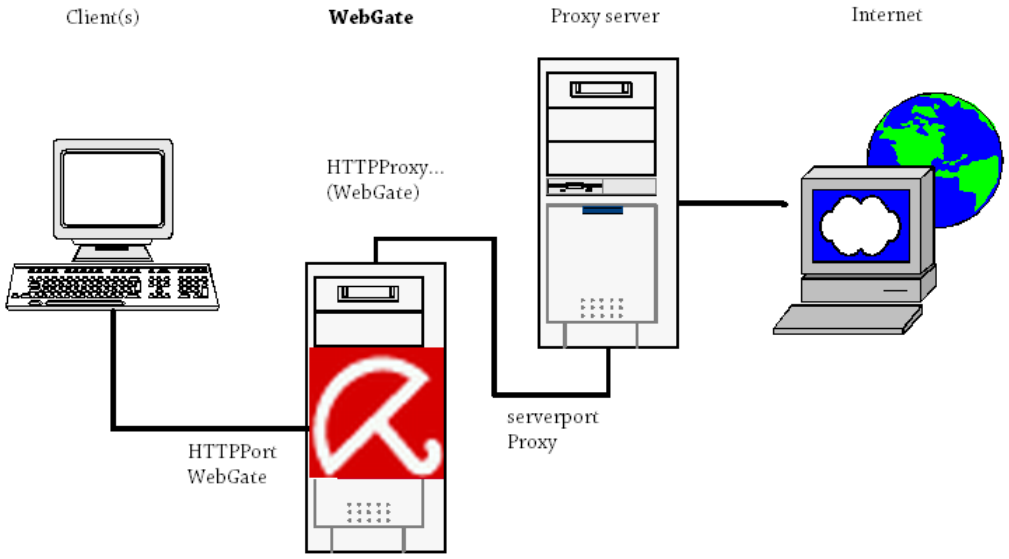
Die tatsächlichen Einstellungen können von den Beispielen abweichen. Für eine korrekte Konfiguration müssen die Einstellungen in avwebgate.conf *mit der Konfiguration des Client-Browsers kompatibel sein.*

WebGate zwischen Client und Proxyserver (Netzwerkkonfiguration 1)

Bei dieser Konfiguration besteht die Gefahr, dass der Proxyserver von schädlicher Software befallen wird. Wenn der Proxyserver vollständig geschützt werden soll (Normalfall), sollte die Netzwerkkonfiguration 2 verwendet werden. Weitere Informationen finden Sie unter *WebGate zwischen Proxyserver und Internet (Netzwerkkonfiguration 2) – Seite 21.*

Sinnvoll ist diese Konfiguration dann, wenn der Proxyserver noch mit anderen Servern verbunden ist und sichergestellt werden muss, dass die Clients nicht infiziert werden. WebGate kann direkt auf dem Proxyserver oder auf einem anderen Computer installiert werden.

WebGate leitet die Client-Anfragen über den Proxyserver an das Internet weiter und prüft die Antworten, die über den Proxyserver aus dem Internet eintreffen. Der Zugriff auf infizierte Dateien einer Website wird gesperrt. Nur nicht infizierte Dateien werden an die Clients weitergeleitet.



Wenn WebGate und Proxyserver auf demselben Computer installiert sind:
Meist ist es einfacher, die Einstellungen des Proxyservers anzupassen und die ursprünglichen Einstellungen für WebGate zu übernehmen. So sind keine Änderungen an den Clients nötig.

Im folgenden Beispiel wird davon ausgegangen, dass der Proxyserver wie folgt konfiguriert ist:

```
host proxy.mycompany.com
serverport 3128
```

Der Proxyserver kommuniziert also mit den Clients über Port 3128.

▶ Installieren Sie WebGate auf dem Computer „proxy.mycompany.com“.

▶ Nehmen Sie in avwebgate.conf die folgenden Einstellungen vor (Beispiel):

```
HTTPPort 3128
```

↳ Die Clients kommunizieren jetzt bei HTTP- und FTP-Anfragen über WebGate und nicht direkt über den ursprünglichen Proxyserver. Die Browsereinstellungen der Client-Computer dürfen nicht verändert werden.

▶ Geben Sie in avwebgate.conf die folgenden Werte ein (Beispiel):

```
HTTPProxyServer 127.0.0.1
HTTPProxyPort 8080
```

↳ WebGate leitet die HTTP- und FTP-Anfragen an den Port 8080 des lokalen Computers (localhost) weiter.

▶ Ändern Sie den Port des ursprünglichen Proxyservers in den Wert `HTTPProxyPort` (in avwebgate.conf), damit er mit WebGate kommunizieren kann. Beispiel:

```
serverport 8080
```

Wenn WebGate auf dem Proxyserver selbst installiert ist:

▶ Stellen Sie sicher, dass WebGate – wie im obigen Beispiel – nicht über den gleichen Serverport antwortet.

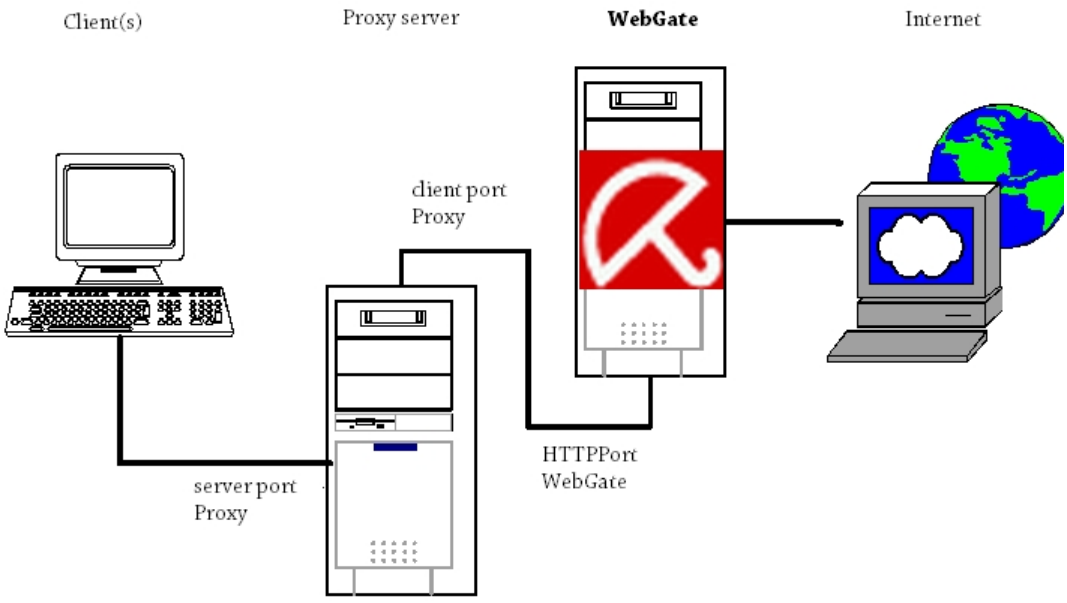
Es ist auch möglich, WebGate auf einem anderen Computer als dem Proxyserver zu installieren. Die Einstellungen müssen entsprechend geändert werden.

Ein Client kann in dieser Netzwerkkonfiguration auch Proxyserver sein (z. B. bei der Installation von WebGate zwischen zwei Proxys).

WebGate zwischen Proxyserver und Internet (Netzwerkkonfiguration 2)

Wenn bereits ein Proxyserver verwendet wird, ist es sinnvoll, WebGate zwischen Proxy und Internet zu installieren. Dadurch kann schädliche Software vom Proxyserver abgefangen werden. WebGate kann direkt auf dem Proxyserver oder auf einem anderen Computer installiert werden.

WebGate leitet die Anfragen der Clients über den Proxy an das Internet weiter und prüft die aus dem Internet eintreffenden Antworten. Der Zugriff auf infizierte Dateien einer Website wird gesperrt. Nur nicht infizierte Dateien werden über den Proxyserver an die Clients weitergeleitet.



In diesem Beispiel wird von der folgenden Konfiguration des Proxyservers ausgegangen:

```
host proxy.mycompany.com
serverport 3128
```

Der Proxyserver antwortet also über Port 3128.

▶ Nehmen Sie in avwebgate.conf die folgenden Einstellungen vor (Beispiel):

```
HTTPPort 8080
```

▶ Konfigurieren Sie den Proxyserver so, dass er Anfragen nicht direkt an das Internet, sondern an WebGate (z. B. an Port 8080) sendet. Dieser Port muss mit dem Wert von `HTTPPort` in avwebgate.conf übereinstimmen.

– *Beispiel für die Konfiguration eines Squid-Proxyservers:*
Bei dieser Konfiguration muss zuerst WebGate und dann der Proxyserver gestartet werden. Der Squid-Proxyserver muss alle Anfragen an WebGate (übergeordneter Proxy) weiterleiten. Deshalb müssen Sie die Squid-Konfigurationsdatei squid.conf wie folgt konfigurieren:

```
cache_peer proxy.mycompany.com parent 8080 0 no-query
no-digest default
acl all src all
never_direct allow all
```

Wenn WebGate auf dem Proxyserver installiert ist:

▶ Stellen Sie sicher, dass WebGate und der Proxyserver nicht über die gleichen Serverports kommunizieren, wie es im obigen Beispiel der Fall ist.

Fordert ein Client Daten an, die bereits im Cache des Proxyservers vorliegen, erhält er seine Daten direkt von dort. Diese Daten werden nicht geprüft, bis der Cache geleert wird. Dadurch besteht ein gewisses Risiko, weil ein neuer Virus „eingeschleppt" und an Clients weitergegeben werden könnte, selbst wenn die VDFs aktualisiert wurden.

Wenn Sie den Port des Proxyservers ändern, müssen Sie die Einstellungen der Client-Browser, die auf den Proxyserver zugreifen, entsprechend anpassen.
Meist ist es einfacher, wie im obigen Beispiel die Proxy-Einstellungen beizubehalten und die Einstellungen von WebGate anzupassen.

4.2 FTP-Verkehr überwachen

WebGate lässt sich auch als **echter** FTP-Proxy einsetzen, der die über FTP-Clients übertragenen Daten prüft und ggf. sperrt. Dabei werden sowohl Downloads als auch Uploads geprüft.

▶ Stellen Sie in avwebgate.conf den Port ein, über den WebGate mit FTP-Clients kommuniziert:

```
FTPPort 2121
```

FTP-Clients können nun über WebGate mit FTP-Servern kommunizieren, d. h. die Clients bauen keine direkte Verbindung zu den FTP-Servern auf, sondern zu WebGate. Damit WebGate stellvertretend eine Verbindung zu einem FTP-Server aufbauen kann, muss die Adresse bzw. der Name des FTP-Servers bekannt sein. Diese Information muss vom FTP-Client bei der Anmeldung mit dem Befehl USER an WebGate übermittelt werden:

```
USER <Benutzername>@<Host>[:<Port>]
```

Anders als beim direkten Verbindungsaufbau zum FTP-Server muss bei der Verbindung über WebGate neben dem für die Anmeldung verwendeten Benutzernamen zusätzlich der Hostname – durch ein @-Zeichen vom Benutzernamen getrennt – oder die IP-Adresse (optional mit Port) des FTP-Servers übermittelt werden.

Beispiel

Das folgende Beispiel veranschaulicht den Anmeldevorgang bei Verwendung eines standardmäßigen UNIX-FTP-Clients:

Annahme: WebGate wird auf einem Computer mit der IP-Adresse `192.168.0.1` ausgeführt und nimmt an Port 2121 Verbindungsanfragen von FTP-Clients entgegen. Es soll eine Verbindung zu einem Remote-FTP-Server mit der IP-Adresse `10.0.0.1`, dem Benutzernamen „foo“ und dem Passwort „bar“ hergestellt werden.

```
$ ftp 192.168.0.1 2121
Connected to 192.168.0.1.
220 AntiVir WebGate FTP proxy. Login with
<Benutzername>@<Host>[:<Port>]
Name (192.168.0.1:user): foo@10.0.0.1
331 Password required for foo.
Password: bar
230 User foo logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Nach der Anmeldung kann der FTP-Client wie gewohnt, d. h. genauso wie ohne WebGate, verwendet werden. WebGate fungiert jetzt als Proxy zwischen FTP-Client und FTP-Server und prüft die übertragenen Daten.

Bei vielen FTP-Clients ist es möglich, einen FTP-Proxy zu konfigurieren. Dadurch wird WebGate für den Benutzer gewissermaßen transparent, d. h. bei der Anmeldung gibt es aus Sicht des Benutzers keine Unterschiede bei der Verwendung des FTP-Clients mit oder ohne Proxy.

Optional erlaubt WebGate auch die Verwendung eines übergeordneten FTP-Proxys. Dieser kann in avwebgate.conf z. B. wie folgt angegeben werden:

```
FTPProxyServer 127.0.0.1
FTPProxyPort 21
```

In diesem Fall kommuniziert WebGate nicht direkt mit dem FTP-Server, sondern mit dem angegebenen übergeordneten FTP-Proxy. Auf diese Weise lassen sich mehrere FTP-Proxyserver hintereinander schalten.

Um Client-Timeouts bei der Übertragung großer Dateien zu vermeiden, sendet WebGate Keepalive-Meldungen an den Client. Als Zeitintervall wird der Wert von `RefreshInterval` oder – falls dieser 0 ist – der Wert von `KeepaliveInterval` verwendet.

Außerdem sendet WebGate im eingestellten `KeepaliveInterval` „NOOP"-Befehle an den Server, um beim Senden und Empfangen großer Dateien zum bzw. vom Client die Verbindung mit dem Server aufrechtzuerhalten.

4.3 Einbindung über die ICAP-Schnittstelle

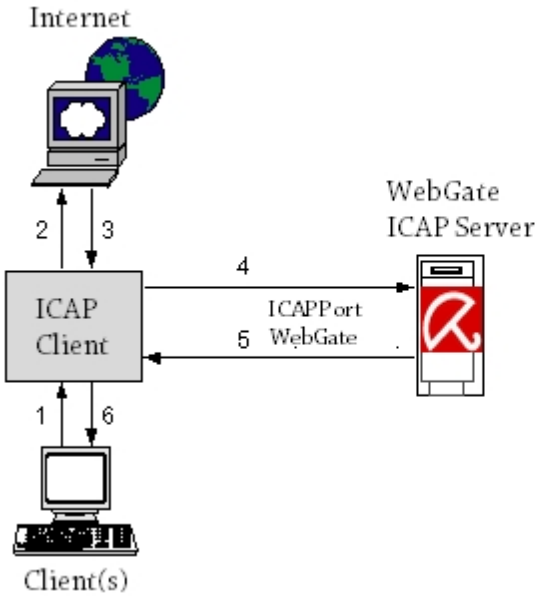
Falls bereits ein Cache-Server mit ICAP-Unterstützung im Netzwerk vorhanden ist, bietet sich die Einbindung von WebGate über die ICAP-Schnittstelle an. Auch in dieser Betriebsart kann WebGate sowohl eingehende (RESPMOD) als auch ausgehende (REQMOD) Dateien prüfen und ggf. sperren.

▶ Legen Sie in avwebgate.conf den Port fest, über den WebGate mit dem ICAP-Client kommuniziert:

```
ICAPPort 1344
```

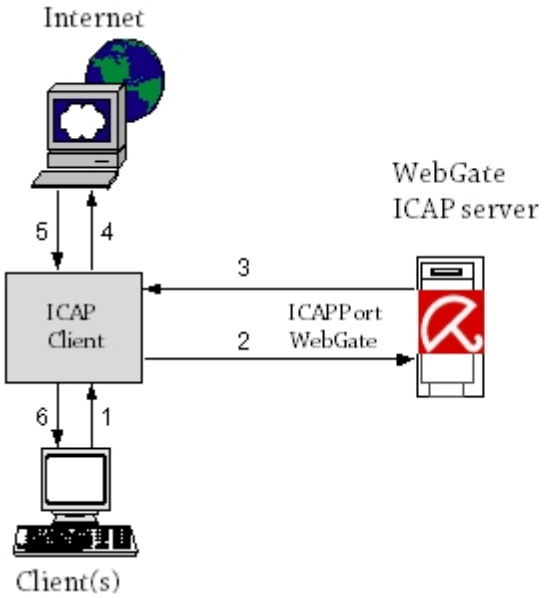
Eingehenden Datenverkehr prüfen (Modifikation von Antworten)

Vom ICAP-Client wird eine HTTP-Antwort zur Prüfung an WebGate (ICAP-Server) gesendet. Sind die Daten nicht infiziert, werden sie an den ICAP-Client zurückgesendet und von diesem an den Client weitergeleitet. Wird die Antwort (z. B. aufgrund eines Virenfunds) gesperrt, generiert WebGate aus der passenden HTML-Vorlage eine HTML-Seite, die an den ICAP-Client gesendet wird. Diese Seite wird anstatt der ursprünglich vom Server empfangenen Antwort an den Client weitergeleitet.



Ausgehenden Datenverkehr überwachen (Modifikation von Anforderungen)

Vom ICAP-Client wird eine HTTP-Anforderung zur Prüfung an WebGate (ICAP-Server) gesendet. Sind die Daten nicht infiziert, werden sie an den ICAP-Client zurückgesendet und von diesem an den Zielserver weitergeleitet. Wird die Anforderung (z. B. aufgrund eines Virenfunds) gesperrt, generiert WebGate aus der passenden HTML-Vorlage eine HTML-Seite, die an den ICAP-Client gesendet wird. In diesem Fall wird die ursprüngliche Anforderung nicht zum Server weitergeleitet.



Weitere Informationen darüber, wie Sie einen ICAP-Server einbinden können, finden Sie in der Dokumentation des ICAP-Clients.

4.4 Konfigurationsdateien

In diesem Abschnitt wird der Inhalt der Konfigurationsdateien von Avira AntiVir WebGate beschrieben:

- /etc/avira/avwebgate.conf – Produktkonfiguration
- /etc/avira/avwebgate-scanner.conf – Scanner-Konfiguration
- /etc/avira/avupdate-webgate.conf – Updater-Konfiguration

Das Programm wird mit Standardeinstellungen ausgeliefert, die für viele Prozesse wichtig sind. Einige Optionen können durch das Zeichen # am Anfang der Zeile deaktiviert (auskommentiert) oder aber mit Standardeinstellungen belegt sein. Sie lassen sich durch Entfernen des Zeichens # bzw. durch Ändern der Werte aktivieren.

4.4.1 Produktkonfiguration in avwebgate.conf

Dieser Abschnitt enthält eine kurze Beschreibung der Einträge in /etc/avira/avwebgate.conf. Die Einstellungen beeinflussen nur das Verhalten von Avira AntiVir WebGate, nicht aber das der anderen Avira AntiVir-Programme. Sie hängen zum Teil von der Grundkonfiguration ab, in der WebGate ausgeführt werden soll (siehe HTTP-Verkehr überwachen – Seite 18).

Proxy-Einstellungen

Diese Einstellungen legen fest, welche Ports von WebGate überwacht und welche Verbindungen akzeptiert werden. Wenn keine Optionen konfiguriert sind, überwacht WebGate nur HTTP-Verbindungen.

HTTPPort **Port für die Überwachung von HTTP-Verbindungen:**
Diese Einstellung legt den Port fest, auf dem WebGate auf HTTP-Anforderungen von Client- oder Proxy-Computern reagiert. Je nach Konfiguration können hier unterschiedliche Einstellungen notwendig sein (siehe HTTP-Verkehr überwachen – Seite 18).
Voreingestellt:

```
HTTPPort [Host_IP_oder_Name:]8080
```

*Wir empfehlen, von außerhalb Ihres Netzwerks **keinen Zugriff** auf WebGate zu erlauben. WebGate sollte also nur mit der internen Netzwerkschnittstelle verbunden werden. Wenn Sie WebGate als übergeordneten Proxy auf einem Computer installieren, auf dem bereits ein Proxyserver vorhanden ist, empfehlen wir z. B. die folgenden Einstellungen:*

```
HTTPPort 127.0.0.1:8080
```

Wenn weder Hostname noch IP-Adresse angegeben sind, wird der Port allen Schnittstellen zugeordnet.

FTPPort **Port für die Überwachung von FTP-Verbindungen:**
WebGate kann auch **echte** FTP-Verbindungen überwachen. Anders als bei „FTP über HTTP“ kommuniziert WebGate hier über FTP mit dem Client. Dieser Eintrag legt den Port fest, über den WebGate FTP-Verbindungen zu Client-Computern

oder zum FTP-Proxyserver herstellt.

Beispiel:

```
FTPPort [Hostname_oder_IP:]2121
```

Voreingestellt:

```
NONE
```

ICAPPort

Port für ICAP-Support:
WebGate kann über die ICAP-Schnittstelle (als ICAP-Server) eingebunden werden. Dieser Eintrag legt den Kommunikationsport fest, über den WebGate mit ICAP-Clients kommuniziert.

Beispiel:

```
ICAPPort [Hostname_oder_IP:]1344
```

Voreingestellt:

```
NONE
```

Max Connections

Maximal zulässige Anzahl von Verbindungen:
Die maximale Anzahl gleichzeitiger Verbindungen, die WebGate zulässt. Der Wert beschränkt die Anzahl der Verbindungen bzw. Threads, die gleichzeitig möglich sind.

Wertebereich: Minimum 0, Maximum 15000

Beispiel:

```
MaxConnections 1000
```

Voreingestellt:

```
MaxConnections 1024
```

Bei der Einstellung `0` lässt WebGate eine unbegrenzte Anzahl gleichzeitiger Verbindungen zu.

Verbindungseinstellungen

HTTPProxy

Einstellungen für HTTP-Proxyserver:
Diese Einstellungen sind nur in Netzwerkkonfiguration 1 wirksam. Bei der Installation vor einem Proxyserver benötigt WebGate nämlich folgende Informationen:

- `HTTPProxyServer:` Name oder IP-Adresse des Proxyservers
- `HTTPProxyPort:` Port des Proxyservers
- `HTTPProxyUsername,HTTPProxyPassword:` Anmeldename und Passwort für den Proxyserver (falls erforderlich)

Beispiel:

```
HTTPProxyServer [Hostname|IP]
HTTPProxyPort 3128
HTTPProxyUsername Benutzername
HTTPProxyPassword Passwort
```

Voreingestellt:

```
HTTPProxyPort 3128
```

Wertebereich: Minimum 0, Maximum 65535

FTPProxy

Einstellungen für FTP-Proxyserver:
Wenn WebGate als FTP-Proxy betrieben wird (siehe Option `FTPPort`), kann ein übergeordneter Proxy für FTP-Verbindungen festgelegt werden.

Wertebereich: Minimum 0, Maximum 65535

Beispiel:

```
FTPProxyPort 2121
```

Voreingestellt:

```
FTPProxyPort 21
```

Umgebungseinstellungen

User
Group

Benutzer und Gruppe wechseln:
Nach dem Start kann WebGate seinen Prozess von einem anderen Benutzer oder einer anderen Gruppe ausführen lassen. WebGate sollte nicht als **root** ausgeführt werden. Geben Sie die Benutzer- und Gruppen-IDs ein, die WebGate nach dem Start annehmen soll (dadurch gibt WebGate seine **root**-Berechtigung ab).

Voreingestellt:

```
User nobody
Group antivir
```

WebGate muss zunächst als root gestartet werden. Wenn Sie diesen Parameter ändern möchten, müssen Sie in der Datei /etc/avira/avwebgate.conf *für* `User` *und* `Group` *die entsprechenden Werte angeben und selbige auch in der Datei* /etc/avira/webgate-scanner.conf *ändern.*

ScannerListen
Address

Speicherort des Scanners:
WebGate startet den SAVAPI-Daemon nicht mehr. Stattdessen wird über einen UNIX-Socket eine Verbindung zu einer laufenden Instanz hergestellt.

Voreingestellt:

```
ScannerListenAddress /var/run/avwebgate/scanner
```

Wenn Sie diesen Parameter ändern, müssen Sie auch den Wert für `ListenAddress` *in* /etc/avira/avwebgate-scanner.conf *ändern. Weitere Informationen finden Sie unter* *Scanner-Konfiguration in avwebgate-scanner.conf – Seite 40.*

Temporary
Dir

Temporäres Verzeichnis:
Der Name des temporären Verzeichnisses kann geändert werden. Voreingestellt ist: `/tmp`. In diesem Verzeichnis werden z. B. die Dateien während der Prüfung abgelegt.

Voreingestellt:

```
TemporaryDir /tmp
 (/var/tmp für Solaris-Binärdateien)
```

CacheDir **Cache Verzeichnis:**

Verzeichnis, in dem die RTPS und Webprotector Cache Dateien gespeichert werden.

Beispiel:

```
CacheDir /home/cache
```

Voreingestellt:

```
CacheDir /var/cache/webgate
```

EmailTo **Email-Nachrichten:**
Avira AntiVir WebGate kann Emails mit zusätzlichen Informationen (z. B. über eine betroffene Datei) versenden, wenn ein Virus oder ein unerwünschtes Programm erkannt wird. Für diese Option gibt es keine Standardeinstellung. Damit Emails verschickt werden können, muss eine Empfängeradresse angegeben werden.

Beispiel:

```
EmailTo root@localhost
```

Voreingestellt:

```
NONE
```

Protokollierungseinstellungen

Syslog Facility **Syslog-Facility:**
WebGate sendet bei allen wichtigen Vorgängen eine Meldung an den syslog-Daemon. Sie können festlegen, welche Facility diesen Meldungen zugeordnet wird.

Beispiel:

```
SyslogFacility home
```

Voreingestellt:

```
SyslogFacility user
```

Wie detailliert diese Meldungen sind, hängt von der mit `LogLevel` eingestellten Protokollierungsebene ab.

LogFile **Pfad und Name der Logdatei:**
Alle wichtigen Vorgänge in WebGate werden von einem syslog-Daemon protokolliert. Sie können eine zusätzliche Logdatei verwenden, indem Sie ihren vollständigen Pfad angeben.

Beispiel:

```
LogFile /var/log/avwebgate.log
```

Voreingestellt:

```
NONE
```

LogLevel

Protokollierungsebene:
Diese Option legt die Protokollierungsebene für WebGate-Meldungen fest (mögliche Werte: 0 bis 7). Je höher die Ebene, desto mehr Informationen werden protokolliert. Die Werte entsprechen den UNIX-Standardebenen, die in syslog verwendet werden:

- `0: Keine Meldungen`
- `1: Alarme`
- `2: Alarme und Fehler`
- `3: Alarme, Fehler und Warnungen`
- `4: Alarme, Fehler und Warnungen`
- `5: Alarme, Fehler und Warnungen`
- `6: Alarme, Fehler, Warnungen und Informationen`
- `7: Alarme, Fehler, Warnungen, Informationen und Debug-Meldungen`

Wertebereich: Minimum 0, Maximum 7

Beispiel:

```
LogLevel 3
```

Voreingestellt:

```
LogLevel 4
```

DebugLevel

Debug-Ausgabe:
Mit dieser Einstellung wird die Detailebene für die Debug-Ausgabe festgelegt (`LogLevel 7`).

Wertebereich: Minimum 0, Maximum 7

Beispiel:

```
DebugLevel 3
```

Voreingestellt:

```
DebugLevel 4
```

Einstellungen der HTTP-Verbindung

AllowHTTPS Tunnel

HTTPS-Tunnel zulassen:
WebGate erlaubt das Tunneln von SSL-Verbindungen (HTTPS). Da die Daten verschlüsselt sind, werden sie nicht geprüft. WebGate greift nicht in die Transaktion ein, sondern leitet lediglich die Daten weiter. Daher kann WebGate auch nicht nachprüfen, ob oberhalb von SSL tatsächlich HTTP übertragen wird. Aus diesem Grund werden nur Verbindungen zu den Ports 443 (HTTPS) und 563 (SNEWS) zugelassen.

Syntax:

```
AllowHTTPSTunnel "YES|NO"
```

Voreingestellt:

```
AllowHTTPSTunnel NO
```

*Die über den HTTPS-Tunnel übertragenen Daten werden von WebGate **nicht** geprüft.*

AllowedHTTP ConnectPorts

Verbindungen mit SSL-Verschlüsselung tunneln:
Wenn Sie HTTPS-Verbindungen zu nicht standardmäßigen Ports zulassen möchten, können Sie die gewünschten Ports in diese Liste aufnehmen. Die einzelnen Ports müssen durch Kommas oder Leerzeichen voneinander getrennt werden.

Voreingestellt:

```
AllowedHTTPConnectPorts 443, 563
```

AddX ForwardedFor Header

Header-Analyse:
Sind in einem Netzwerk mehrere Proxyserver hintereinander geschaltet, kann ein nachgelagerter Proxyserver keine auf Client-IP-Adressen basierenden Auswertungen durchführen, da die Anforderungen aus seiner Sicht alle von derselben Adresse stammen, nämlich vom vorgelagerten Proxy. Der nachgelagerte Proxyserver kennt also nur die Adresse seines unmittelbaren Kommunikationspartners, nicht aber die Adresse des Computers, von dem die Anforderung ursprünglich stammt.

Ist die Option `AddXForwardedForHeader` aktiviert, ergänzt WebGate die HTTP-Anforderung um ein zusätzliches Header-Feld (X-Forwarded-For) oder fügt die IP-Adresse des Clients hinzu, von dem die Anforderung empfangen wurde. Auf diese Weise kann WebGate nachgelagerten Proxyservern die Client-IP-Adresse übermitteln. Diese können das Header-Feld anschließend auswerten und die darin enthaltenen indirekten Daten z. B. für Zugriffssteuerungsmechanismen oder die Protokollierung verwenden.

Die Option ermöglicht beispielsweise die Nutzung der ACLs eines Squid-Proxys, der von WebGate als übergeordneter Proxy konfiguriert wurde. Der übergeordnete Proxy muss natürlich über die entsprechende Funktionalität zur Header-Auswertung verfügen.

Syntax:

```
AddXForwardedForHeader "YES|NO"
```

Voreingestellt:

```
AddXForwardedForHeader NO
```

RemoveX ForwardedFor Header

Header-Analyse:
Ist die Option `RemoveXForwardedForHeader` aktiviert, entfernt WebGate den X-Forwarded-For Header aus der empfangenen Anforderung.

Syntax:

```
RemoveXForwardedForHeader "YES|NO"
```

Voreingestellt:

```
RemoveXForwardedForHeader NO
```

AddViaHeader

Header-Analyse:
Wenn WebGate im ICAP Modus verwendet wird, fügt diese Option einen Via-

Header hinzu.

Syntax:

```
AddViaHeader "YES|NO"
```

Voreingestellt:

```
AddViaHeader NO
```

AddIcapDate Header

Header-Analyse:
Wenn WebGate im ICAP Modus verwendet wird, fügt diese Option einen Date-Header hinzu. Voreingestellt sendet WebGate keine Date-Header wenn es auf eine ICAP-Anfrage antwortet. Setzen Sie die Option auf "YES", um das Versenden der Datumsangabe zu ermöglichen.

Syntax:

```
AddIcapDateHeader "YES|NO"
```

Voreingestellt:

```
AddIcapDateHeader NO
```

Beispiel:

```
AddIcapDateHeader YES
```

Einstellungen zum Verhindern von Timeouts

Diese Einstellungen legen fest, wie WebGate die Verbindung zum Client während der Verarbeitung der Anforderung aufrechterhält.

Refresh/ Redirect/ Keepalive Interval

Client-Timeouts bei großen Downloads verhindern:
Einige Browser und Proxys geben eine Fehlermeldung aus, wenn sie nach einer gewissen Wartezeit keine Daten empfangen (Timeout). Wenn WebGate ein größeres Datenpaket herunterlädt und überprüft, kann es zu solchen Timeout-Meldungen kommen.

WebGate bietet verschiedene Möglichkeiten, um Timeouts zu verhindern.
Die Einträge werden in Sekunden angegeben.

- Wenn der Client ein Browser ist, sendet WebGate eine HTML-Seite mit dem aktuellen Fortschritt, die in regelmäßigen Abständen aktualisiert wird.

Refresh Interval

Refresh Intervall

Wertebereich: Minimum 0, Maximum 3600

Beispiel:

```
RefreshInterval 1800
```

Voreingestellt:

```
RefreshInterval 0
```

- Wenn die Option `RefreshInterval` deaktiviert wird oder der Client kein Browser ist, werden temporäre Umleitungen (HTTP-Redirects) an den Client gesendet. So wird der Client zyklisch zu einer dynamisch generierten URL

umgeleitet, die von WebGate abgefangen wird, um einen Timeout zu verhindern.

Redirect Interval

Redirect Intervall

Wertebereich: Minimum 0, Maximum 3600

Beispiel:

```
RedirectInterval 1800
```

Voreingestellt:

```
RedirectInterval 0
```

- Die obige Methode funktioniert nicht bei jedem Client. Wenn Probleme auftreten, können Sie mit der Option `KeepaliveInterval` veranlassen, dass WebGate in bestimmten Abständen Meldungen an den Client sendet. Der hier angegebene Wert muss kleiner sein als der, der für den Client oder Proxyserver eingestellt ist.

Keepalive Interval

Keepalive Intervall

Wertebereich: Minimum 0, Maximum 3600

Beispiel:

```
KeepaliveInterval 60
```

Voreingestellt:

```
KeepaliveInterval 30
```

- Im vorgegebenen Intervall versendet WebGate erweiterte Header-Daten zum Client. Um die Verbindung aufrechtzuerhalten, versendet WebGate außerdem „no-operation"-Befehle an den Server während des Sendens oder des Empfangs großer Dateien zum bzw. vom Client.

KeepaliveMode

Keepalive Mode

Syntax:

```
KeepaliveMode "trickle|header"
```

Beispiel:

```
KeepaliveMode trickle
```

Voreingestellt:

```
KeepaliveMode header
```

- Wenn die oben beschriebenen Verfahren zur Verhinderung von Timeouts in Ihrer Umgebung nicht umgesetzt werden können oder nicht funktionieren und deshalb Client-Timeouts auftreten, können Sie das Data-Trickling aktivieren, indem Sie in avwebgate.conf die Option `KeepaliveMode` auf `trickle` setzen. WebGate sendet die Daten dann in kleinen Paketen in dem mit `KeepaliveInterval` festgelegten Intervall, bis Download und Überprüfung abgeschlossen sind. Nachdem die Datei heruntergeladen und überprüft wurde, wird sie sofort an den Client gesendet (sofern sie keine infizierten Daten enthält). Unter dem voreingestellt Wert `header` verwendet

WebGate die oben beschriebenen `Refresh`, `Redirect` und `Keepalive` Intervalle.

Data-Trickling sollte NUR verwendet werden, wenn die anderen Methoden zur Verhinderung von Timeouts nicht zum Erfolg führen. Beachten Sie die Risiken und Einschränkungen dieses Verfahrens, bevor Sie diese Funktion aktivieren. Auch wenn WebGate alle Daten überprüft, die an den Client gesendet werden, birgt die trickle-Option ein gewisses Risiko, dass es zu einer Infektion kommt. Das trickle-Intervall kontrolliert das Versenden der Daten mit einer vorgegebenen Geschwindigkeit und einem vorgegebenen Volumen, sodass die Downloadgeschwindigkeit, die am Client gezeigt wird, nicht der tatsächlichen Geschwindigkeit entspricht.

Prüf- und Filtereinstellungen

ArchiveScan

Archive prüfen:
Standardmäßig werden alle Dateien in Archiven beim Zugriff entpackt und überprüft. Dabei gelten die Einstellungen für `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio`.

Es wird empfohlen, diese Optionen **nicht** zu deaktivieren.

Syntax:

```
ArchiveScan "YES|NO"
```

Voreingestellt:

```
ArchiveScan YES
```

ArchiveMax Size

Maximale Größe von archivierten Dateien:
Mit dieser Option lässt sich die Prüfung auf Dateien beschränken, die im entpackten Zustand kleiner als `ArchiveMaxSize` (in Byte) sind. Beim Wert 0 gilt keine Beschränkung.

Syntax:

```
ArchiveMaxSize "positive Zahl|K|M|G"
```

Beispiel:

```
ArchiveMaxSize 1G
```

Voreingestellt:

```
ArchiveMaxSize 2G
```

ArchiveMax Recursion

Maximale Rekursionstiefe:
Wenn rekursive (verschachtelte) Archive geprüft werden, kann die Rekursionstiefe beschränkt werden. Beim Wert 0 werden alle Archive unabhängig von der Rekursionstiefe vollständig entpackt.

Wertebereich: Minimum 0, Maximum 1000

Syntax:

```
ArchiveMaxRecursion "positive Zahl"
```

Beispiel:

```
ArchiveMaxRecursion 10
```

Voreingestellt:

```
ArchiveMaxRecursion 20
```

ArchiveMax Ratio

Maximale Kompressionsrate für Archive:
Mit dieser Option lässt sich die Prüfung auf Archive beschränken, die eine vorgegebene Kompressionsrate nicht überschreiten. Diese Maßnahme schützt vor so genannten „Mail-Bomben“, die beim Entpacken unerwartet viel Speicherplatz belegen würden. Beim Wert 0 werden alle Archive unabhängig von der Kompressionsrate vollständig entpackt.

Wertebereich: Minimum 0, Maximum 1000

Beispiel:

```
ArchiveMaxRatio 100
```

Voreingestellt:

```
ArchiveMaxRatio 150
```

Block Suspicious Archive

Verdächtige Archive sperren:
Ist diese Option aktiviert, werden Archive gesperrt, wenn einer der in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio` festgelegten Grenzwerte überschritten wird.

Ist die Option deaktiviert, werden alle Archive unabhängig von den Einstellungen in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio` weitergeleitet.

Syntax:

```
BlockSuspiciousArchive "YES|NO"
```

Voreingestellt:

```
BlockSuspiciousArchive YES
```

Block Encrypted Archive

Passwortgeschützte Archive sperren:
Ist diese Option aktiviert, werden passwortgeschützte Archive durch WebGate gesperrt.

Syntax:

```
BlockEncryptedArchive "YES|NO"
```

Voreingestellt:

```
BlockEncryptedArchive NO
```

BlockPartial Archive

Aufgeteilte Archive sperren:

Ist diese Option aktiviert, werden Archive gesperrt, die auf mehrere Datenträger verteilt sind.

Syntax:

```
BlockPartialArchive "YES|NO"
```

Voreingestellt:

```
BlockPartialArchive NO
```

BlockArchive Bomb

Archivbomben sperren:

Ist diese Option aktiviert, sperrt WebGate Dateien, bei denen es sich um Archivbomben handeln könnte.

Syntax:

```
BlockArchiveBomb "YES|NO"
```

Voreingestellt:

```
BlockArchiveBomb YES
```

Die in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio` festgelegten Grenzwerte haben keine Auswirkung auf diese Option.

Block Extensions

Bestimmte Dateierweiterungen sperren:
WebGate kann Dateien mit bestimmten Erweiterungen sperren. Die Sperre gilt auch für Dateinamen in Archiven.

Syntax:

```
BlockExtensions "ext1;ext2;ext3"
```

Beispiel:

```
BlockExtensions exe;scr;pif
```

Voreingestellt:

```
NONE
```

Block Categories

URL-Filterung:
Zuerst werden die **Zugriffssteuerungsregeln (ACL)** ausgewertet. Wenn eine Regel das Tunneln einer Anforderung erlaubt, erfolgt keine Sperrung durch URL-Filter. Nicht getunnelte Verbindungen werden – ähnlich wie beim Prüfverhalten – nicht vom URL-Filtermodul blockiert.

Danach erfolgt eine Prüfung durch die **URL-Filterbibliothek von Avira** (LocalFilter). Dabei wird anhand einer Liste bekannter URLs festgestellt, ob eine URL gefährlich ist. Für jede gefährliche URL wird eine der folgenden Kategorien zurückgegeben: Malware (60), Phishing (61), Betrug (63). Ist die zurückgegebene Kategorie in der Konfigurationsoption `BlockCategories` angegeben, wird die Anforderung abgelehnt. Die Avira-URL-Filterbibliothek steht zur Verfügung, wenn eine gültige Lizenz für WebGate oder WebGate Suite vorhanden ist.

Wenn die URL nicht in der Avira-URL-Filterbibliothek enthalten ist oder nicht durch die Konfigurationsdatei blockiert wird, wird die **Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung** (OnlineFilter) verwendet. Diese Bibliothek filtert Anforderungen auf der Grundlage der URL-Kategorie. Diese Funktion steht nur in der Avira AntiVir WebGate Suite zur Verfügung.

Die Kategorien können einzeln oder in Form von Kategoriebereichen angegeben werden. Zur Angabe eines Bereichs verbinden Sie die betreffenden

Kategorienummern mit einem Minuszeichen (-). (4.9 URL-Filterung)

Beispiel:

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

Voreingestellt:

```
NONE
```

Move Concerning FilesTo

Quarantäneverzeichnis:
Gesperrte Dateien werden standardmäßig gelöscht. Sie können jedoch auch ein Quarantäneverzeichnis angeben, in dem sie gespeichert werden sollen.

Syntax:

```
MoveConcerningFilesTo "Pfadangabe"
```

Beispiel:

```
MoveConcerningFilesTo /home/quarantine
```

Voreingestellt:

```
NONE
```

Heuristics Level

Win32-Heuristik:
Mit dieser Option wird die Erkennungsstufe der Win32-Heuristik festgelegt. Zulässige Werte sind `0` (Aus), `1` (Niedrig), `2` (Mittel) und `3` (Hoch).

Wertebereich: Minimum 0, Maximum 3

Syntax:

```
HeuristicsLevel "0|1|2|3"
```

Beispiel:

```
HeuristicsLevel 1
```

Voreingestellt:

```
HeuristicsLevel 2
```

Heuristics Macro

Makrovirus-Heuristik:
Diese Option aktiviert die Heuristik für Makroviren in Dokumenten. Die Option ist standardmäßig aktiviert.

Syntax:

```
HeuristicsMacro "YES|NO"
```

Voreingestellt:

```
HeuristicsMacro YES
```

Detect...

Erkennung weiterer unerwünschter Programme:
Neben Viren gibt es weitere schädliche oder unerwünschte Software. Die Erkennung dieser Software kann mithilfe folgender Optionen erfolgen:

```
DetectADSPY (Voreingestellt YES)
DetectAPPL (Voreingestellt NO)
DetectBDC (Voreingestellt YES)
DetectDIAL (Voreingestellt YES)
```

```
DetectGAME (Voreingestellt NO)
DetectHEUR-DBLEXT (Voreingestellt YES)
DetectJOKE (Voreingestellt NO)
DetectPCK (Voreingestellt NO)
DetectPHISH (Voreingestellt YES)
DetectSPR (Voreingestellt NO)
```

Sie können die Erkennung für alle oben aufgeführten Kategorien aktivieren, indem Sie den folgenden Parameter auskommentieren. Dadurch wird die Erkennung aller unerwünschten Programme aktiviert, d. h. die individuellen Einstellungen der Optionen werden überschrieben.

Syntax:

```
DetectAllTypes "YES|NO"
```

Voreingestellt:

```
DetectAllTypes YES
```

SMC-Einstellungen

GUI...

SSL-Parameter für sichere Kommunikation mit Avira SMC

Diese Optionen müssen für eine sichere Kommunikation mit SMC aktiviert sein:

GuiSupport

GuiSupport

Diese Option ermöglicht die Verwendung der Konsole des Avira Security Management Center (SMC), um mit WebGate in der Remote-Funktion arbeiten zu können.

Syntax:

```
GuiSupport "YES|NO"
```

Voreingestellt:

```
GuiSupport NO
```

GuiCAFile

GuiCAFile

Spezifiziert den Pfad zu der Zertifikatsdatei einer Zertifizierungsstelle, die für die Kommunikation mit SMC verwendet wird.

Syntax:

```
GuiCAFile "Pfadangabe"
```

Beispiel:

```
GuiCAFile  /usr/lib/AntiVir/webgate/gui/cert/
cacert.pem
```

Voreingestellt:

```
NONE
```

GuiCertFile

GuiCertFile

Spezifiziert den Pfad zu der Zertifikatsdatei, die für die Kommunikation mit SMC und für die Datenbankprotokollierung verwendet wird.

Syntax:

```
GuiCertFile "Pfadangabe"
```

Beispiel:

```
GuiCertFile /usr/lib/AntiVir/webgate//gui/cert/
server.pem
```

Voreingestellt:

```
NONE
```

GuiCertPass

GuiCertPass
Das Passwort für die Zertifikatsdatei.

Syntax:

```
GuiCertPass "string"
```

Beispiel:

```
GuiCertPass antivir_default
```

Voreingestellt:

```
NONE
```

Weitere Informationen zu den erweiterten Konfigurationsoptionen finden Sie im Installationsverzeichnis von WebGate.

GuiHostname

GUI Hostname
Der Hostname der GUI wird von dem Kommando `avwg_stats` als Schnittstelle verwendet, um Verbindungen vom SMC abzuhören.

Syntax:

```
GuiHostname host
```

Voreingestellt:

```
GuiHostname 127.0.0.1 oder localhost
```

Einstellungen für die Zugriffssteuerung

Forbidden UserAgents

Bestimmten Benutzeragenten den Zugriff verweigern:
Sie können eine oder mehrere Zeichenfolgen für Benutzeragenten angeben, denen der Zugriff verweigert wird. Dadurch soll vor allem überflüssiger Datenverkehr mit Clients, die Bereichsanforderungen versenden (wie z. B. der BITS – Background Intelligent Transfer Service – von Microsoft), oder mit Streaming-Geräten (wie iTunes von Apple) vermieden werden. Bereichsanforderungen und Datenstreaming werden nur zugelassen, wenn sie in AclConfigFile (siehe unten) angegeben sind.

Beispiel:

```
ForbiddenUserAgents BITS iTunes
```

Voreingestellt:

```
NONE
```

AclConfigFile

Zugriffssteuerungsschema:
Durch die Implementierung eines Squid-ähnlichen Zugriffssteuerungsschemas ist WebGate in der Lage, auch komplexe Regeln zu unterstützen. Um das Zugriffssteuerungsschema verwenden zu können, müssen Sie zunächst eine neue Konfigurationsdatei mit Regeln erstellen, die das gewünschte Verhalten beschreiben, und den Pfad dieser Datei in `AclConfigFile` angeben.

Syntax:

```
AclConfigFile /etc/avira/avwebgate.acl
```

Voreingestellt:

```
NONE
```

4.4.2 Scanner-Konfiguration in avwebgate-scanner.conf

In Version 3 von WebGate wurde eine neue Konfigurationsdatei eingeführt: /etc/avira/avwebgate-scanner.conf. Diese Datei enthält spezielle Konfigurationsoptionen für das neue Scanner-Backend. Die Optionen in dieser Datei brauchen nur in einigen wenigen Ausnahmefällen geändert zu werden.

User, Group

Benutzer, Grupppe:
Wenn Sie eine dieser Optionen ändern, müssen Sie sicherstellen, dass die Dateien avwebgate-scanner.conf und avwebgate.conf die gleichen Werte für diese Option enthalten und dass der betreffende Benutzer nach wie vor auf alle Verzeichnisse und Dateien zugreifen kann. Außerdem müssen Sie die Datei avwg_stats.lck entsprechend anpassen.

Voreingestellt:

```
User nobody
Group antivir
```

Bitte beachten Sie, dass die Option `User,Group` *nicht durch das SMC unterstützt wird. Eine Änderung an diesen Einstellungen unterdrückt die Kommunikation mit dem SMC.*

In /etc/avira/avwebgate-scanner.conf:

- Ändern Sie den Eigentümer bzw. die Gruppe des in `ListenAddress` angegebenen Pfades. (HINWEIS: Die Option setzt sich aus einem Pfad und einer Socket-Datei zusammen. Beenden Sie WebGate, bevor Sie Änderungen vornehmen. Wenn die Socket-Datei existiert, löschen Sie sie und ändern Sie nur den Eigentümer bzw. die Gruppe des Verzeichnisses.)

Wenn Sie an dieser Stelle den Benutzer und/oder die Gruppe ändern, müssen Sie auch die Optionen `User` *und* `Group` *in der WebGate-Konfigurationsdatei* /etc/avira/avwebgate.conf *ändern.*

- Passen Sie die Option `SocketPermissions` an den neuen Benutzer bzw. die neue Gruppe an (siehe unten).

In /etc/avira/avwebgate.conf:

- Ändern Sie die Option `User/Group`.

Socket Permissions

SocketPermissions

Der Eigentümer und die Berechtigungen für den Socket des Scanner-Backends.

Beispiel:

```
SocketPermissions 0600
```

ListenAddress

ListenAddress

Die Optionen `ListenAddress` (in avwebgate-scanner.conf) und `ScannerListenAddress` (in avwebgate.conf) legen fest, wie das Scanner-Backend zu erreichen ist. Beide Optionen müssen auf denselben Pfad verweisen (die Zeichenfolge „unix:“ darf in der Option `ScannerListenAddress` nicht verwendet werden):

```
ListenAddress unix:/var/run/avwebgate/scanner
ScannerListenAddress /var/run/avwebgate/scanner
```

CreateSocket Dir

CreateSocketDir

Wenn diese Option durch aktiviert ist, erstellt SAVAPI Service während des Startvorgangs ein übergeordnetes Verzeichnis für die Socketdatei, wenn der vorgesehene Pfad nicht existiert.

Beispiel:

```
CreateSocketDir 1
```

Voreingestellt:

```
CreateSocketDir 1
```

Wenn die Option CreateSocketDir nicht in der Scanner-Konfigurationsdatei existiert, wird das übergeordnete Verzeichnis der Socketdatei während des Startvorgangs nicht erstellt.

PoolScanners

PoolScanners

Die Anzahl der AntiVir-Scanner im Pool.

Beispiel:

```
PoolScanners 70
```

Voreingestellt:

```
PoolScanners 105
```

Pool Connections

PoolConnections:

Die maximale Anzahl gleichzeitiger Verbindungen, die WebGate für den Scanner-Pool zulässt.

Beispiel:

```
PoolConnections 70
```

Voreingestellt:

```
PoolConnections 192
```

PidDir

PidDir
Legt den Ort der SAVAPI Service PID Datei fest. Es werden nur absolute Pfadangaben akzeptiert. Wenn Sie relative Pfadangaben eingeben, wird SAVAPI mit einer Fehlermeldung beendet.

Beispiel:

```
PidDir /var/temp/webgate
```

Voreingestellt:

```
PidDir /var/temp
```

LogFileName

LogFileName:
Der Name und Pfad der Scanner-Logdatei.

Beispiel:

```
LogFileName /var/log/avwebgate-scanner.log
```

Voreingestellt:

```
LogFileName NONE
```

SyslogFacility

SyslogFacility:
Die zur Anmeldung bei syslog verwendet `Facility`.

Bespiel:

```
SyslogFacility home
```

Voreingestellt:

```
SyslogFacility user
```

ReportLevel

ReportLevel:
Der Scanner kann auf verschiedene Protokollebenen eingestellt werden:

- 0 – Fehler
- 1 – Fehler und Alarme
- 2 – Fehler, Alarme, Warnungen und Informationen
- 3 – Fehler, Alarme, Warnungen, Informationen und Debug-Meldungen

Ein „Alarm“ enthält Informationen über potentiell schädlichen Code.

Beispiel:

```
ReportLevel 1
```

Voreingestellt:

```
ReportLevel 0
```

4.4.3 Updater-Konfiguration in avupdate-webgate.conf

Aktualisierungen stellen sicher, dass die Komponenten von AntiVir WebGate (WebGate, Scanner, VDF und Engine), die für den Schutz vor Viren und unerwünschten Programmen sorgen, stets auf dem neuesten Stand sind.

Mit Avira Updater können Sie die Avira-Software auf Ihrem Computer über die Avira-Update-Server aktualisieren. Um den Aktualisierungsvorgang zu konfigurieren, verwenden Sie die Optionen in /etc/avira/avupdate-webgate.conf, die

weiter unten beschrieben sind. Alle Parameter in avupdate-webgate.conf können über die Befehlszeile an Avira Updater übergeben werden. Beispiel:

– Parameter in avupdate-webgate.conf:

```
temp-dir=/tmp
```

– Befehlszeile:

```
/usr/lib/AntiVir/webgate/avupdate-webgate.bin --temp-
dir=/tmp
```

internet-srvs **internet-svrs:**
Die Liste der Internet-Update-Server.

```
internet-srvs=http://professional.avira-update.com.,
http://professional.avira-update.net
```

master-file **master-file:**
Die master.idx-Datei.

```
master-file=/idx/master.idx
```

install-dir **Installationsverzeichnis:**
Das Installationsverzeichnis für aktualisierte Produktdateien.

```
install-dir=/usr/lib/AntiVir
```

temp-dir **Temporäres Verzeichnis:**
Temporäres Verzeichnis für heruntergeladene Aktualisierungsdateien.

```
temp-dir=/tmp/avira_update/webgate
```

Email-Aktualisierungsberichte einstellen

Alle Berichte über AntiVir-Aktualisierungen werden an die Email-Adressen gesendet, die in avupdate-webgate.conf angegeben sind:

mailer **Emails:**

Emails können via `smtp` oder `sendmail` gesendet werden:

```
mailer=mutt
```

smtp... **SMTP-Verbindung:**

Authentifizierung der SMTP-Verbindung. Aktivieren Sie die Option `auth-method` und geben Sie den SMTP-Server, den Port, den Benutzer und das Passwort an.

```
auth-method=password
smtp-user=<Ihr_Benutzername>
smtp-password=<Ihr_Passwort>
smtp-server=<Servername>
smtp-port=25
```

notify-when **Benachrichtigungen:**

Email-Benachrichtigungen können auf drei Werte eingestellt werden:

- 0 – Es werden keine Email-Benachrichtigungen gesendet.
- 1 – Email-Benachrichtigungen werden in folgenden Fällen gesendet: „Aktualisierung erfolgreich“, „Aktualisierung nicht erfolgreich“ und „Auf dem neuesten Stand“.
- 2 – Eine Email-Benachrichtigung wird nur bei „Aktualisierung nicht erfolgreich“ gesendet.
- 3 – Eine Email-Benachrichtigung wird nur bei „Aktualisierung erfolgreich“ gesendet (Standardeinstellung).

Beispiel:

```
notify-when=1
```

Voreingestellt:

```
notify-when=3
```

email-to **Email-Empfänger:**

Der Empfänger der Email-Benachrichtigungen.

Beispiel:

```
email-to root@localhost
```

Voreingestellt:

```
email-to root@localhost
```

Verbindungseinstellungen für Aktualisierungen

proxy... **Proxy-Einstellungen:**

Wenn ein HTTP-Proxyserver verwendet wird, müssen für Aktualisierungen über das Internet Einstellungen für die Proxy-Konfiguration festgelegt werden.

```
proxy-host=
proxy-port=
proxy-username=
proxy-password=
```

Voreingestellt:

```
NONE
```

user-agent **Benutzeragent:**

Legt die Zeichenfolge für den Benutzeragenten (`--user-agent`) fest, die zum HTTP- Server weitergeleitet wird.

Voreingestellt:

```
@AUVI@1.0;<product_name>-UpdateCP/<updater version>
(<license types>;<products>; <language>; AVE <engine
version>; VDF <VDF version>; <operating system name>;
<operating system details>; <country>; <serial>; <li-
cense serials>; <operating system language>; )
```

Voreingestellt für `<product_name>` ist `AntiVir`. Ist die Option `--product-name-file` festgelegt oder existiert die Standarddatei productname.dat, wird

<product name> durch den Inhalt der entsprechenden Datei ersetzt.

Beispiele:

- Wenn die Option --product-name-file nicht angegeben ist:

```
@AUVI@1.0;AntiVir-UpdateCP/2.0.3.6 (SAVXE;
SAVAPILINUX_GLIBC24_X86_64-EN; EN; AVE 8.2.10.52; VDF
7.11.28.140; LINUXX86_64 2.6.38-13-GENERIC; DISTRO RE-
LEASE SQUEEZE/SID GLIBC 2.13;EN_US.UTF-8;
A182365FA39EE0327E3A4918B0358475; 2100133080-ASRTE-
0000001; EN_US.UTF-8; )
```

- Wenn die Standarddatei productname.dat wirksam ist:

```
@AUVI@1.0;WEBGATE3.3-UpdateCP/2.0.3.6 (SAVXE;
SAVAPILINUX_GLIBC24_X86_64-EN; EN; AVE 8.2.10.52; VDF
7.11.28.140; LINUXX86_64 2.6.38-13-GENERIC; DISTRO RE-
LEASE SQUEEZE/SID GLIBC 2.13;EN_US.UTF-8;
A182365FA39EE0327E3A4918B0358475; 2100133080-ASRTE-
0000001; EN_US.UTF-8; )
```

product-name-file **Product-name-Datei**

Gibt die Datei an, in welcher der Produktname gespeichert ist (z.B. WEBGATE3.3). Der Dateipfad ist relativ zur binären Aktualisierungsspeicherstelle. Der Produktname wird in das Feld <product_name> der Zeichenfolge --user-agent eingefügt.

Die Datei muss lesbar sein und den Produktnamen in Form einer druckbaren ASCII-Zeichenkette enthalten. Es dürfen keine Leerzeichen enthalten sein und die maximale Länge darf 64 Zeichen nicht überschreiten. Anderenfalls wird eine Fehlermeldung ausgegeben und der Aktualisierungsprozess wird gestoppt.

Ist keine product-name-Datei spezifiziert und die Standarddatei productname.dat existiert nicht, werden in der Zeichenfolge Benutzeragent (--user-agent) keine Änderungen vorgenommen.

Der voreingestellte Wert: productname.dat enthält folgenden Text: WEBGATE3.3

Beispiel:

```
avupdate.bin --product-name-file=my_product_name.dat
```

Logdatei-Einstellungen

log **Logdatei**

Geben Sie den vollständigen Pfad und Namen der Datei an, in die AntiVir Updater seine Log-Meldungen schreibt.

```
log=/var/log/avupdate-webgate.log
```

log-append **Logdatei ergänzen**

Die Logdatei wird standardmäßig überschrieben. Mit dieser Option können Sie veranlassen, dass Meldungen an das Ende der Logdatei angefügt werden.

```
log-append
```

Einstellungen für Intranet-Aktualisierungen

Wenn Sie statt der voreingestellten Aktualisierung über das Internet ein Update über das Intranet bevorzugen, müssen Sie einige Parameter in der Konfigurationsdatei avupdate-webgate.conf vornehmen, oder selbige in der Kommandozeile eingeben:

`intranet-srvs`

Mit dem Avira Internet Update Manager (IUM) können Sie für eine Vielzahl Ihrer Aviraprodukte automatische Updates bereitstellen lassen. Die einzelnen Clientrechner in Ihrem Netzwerk müssen die Updates nicht selber über das Internet laden, sondern können die Produkte bequem über Ihr Intranet aktualisieren. Weitere Informationen entnehmen Sie bitte dem IUM-Handbuch. (http://www.avira.com).

Legt eine Liste der IUM Server, die durch Komma getrennt werden, fest

`product-root`

Legt das Verzeichnis für die Aktualisierung auf dem IUM Server fest (set to `/update`)

`intranet`

Legt fest, dass die Aktualisierung statt über das Internet durch das Intranet erfolgt.

Beispiel:

```
intranet-svrs=http://iumserver:7080
product-root=/update
intranet
```

Einstellungen für Fallback-Aktualisierungsserver

Wenn Sie einen Fallback-Aktualisierungsserver einrichten möchten, zum Beispiel für den Fall, dass der Intranetserver nicht ordnungsgemäß arbeitet und Sie doch über das Internet aktualisieren möchten, können Sie mithilfe der Option `peak-handling-srvs` in der Konfigurationsdatei oder in der Kommandozeile, diesen einrichten. Die Option folgt der gleichen Syntax wie `intranet-srvs`.

Beispiel:

`peak-handling-srvs=http://profpeak.avira-update.com`

Integration in Avira Security Management Center (SMC)

Damit Sie Aktualisierungen über das Avira Security Management Center (SMC) konfigurieren können, müssen Sie dem SMC-Repository das Paket mit dem Aktualisierungs-Plugin hinzufügen. Danach steht das neue Produkt „Avira Updater“ auf Computern, die über das SMC verwaltet werden, für Installationszwecke zur Verfügung.

Das Produkt „Avira Updater“ ermöglicht die Konfiguration von Aktualisierungen für alle Produkte, die auf SMC-Computern installiert sind. Weitere Informationen finden Sie in der SMC-Dokumentation.

Wenn Sie die Optionen für `User/Group` *geändert haben, wird die Kommunikation mit dem SMC unterdrückt.*

4.4.4 Konfiguration der Zugriffssteuerung in avwebgate.acl

In WebGate ist ein Zugriffssteuerungsschema implementiert, das eine Untermenge von Squid darstellt.

Mithilfe dieser Funktion ist es möglich, Regeln aufzustellen, die ein Tunneln bestimmter Anforderungs- und Antworttypen ermöglichen. Dies ist besonders hilfreich, wenn Streaming-Inhalte oder Benutzeragenten unterstützt werden sollen, die mit HTTP-Bereichsanforderungen arbeiten.

Das Zugriffssteuerungsschema wird in einer eigenen Datei gespeichert, die im Parameter `AclConfigFile` in /etc/avira/avwebgate.conf definiert ist.

In der Datei /etc/avira/avwebgate.acl.example finden Sie einige Beispiele.

4.5 Vorlagenkonfiguration

Wenn Sie eine gültige Lizenzdatei besitzen, können Sie die von Avira AntiVir WebGate zu Benachrichtigungszwecken generierten Webseiten und Emails anpassen. Sie werden von WebGate z. B. dann versendet, wenn Viren oder unerwünschte Programme gefunden wurden. Zur Verfügung stehen die Vorlagen *alert, blocked, error* und *progress*.

Sie werden normalerweise im Verzeichnis /usr/lib/AntiVir/webgate/templates erstellt und gespeichert. Mit dem folgenden Eintrag in /etc/avira/avwebgate.conf kann auch ein anderes Verzeichnis bestimmt werden:

Syntax:

```
/usr/lib/AntiVir/webgate/avwebgate.bin
  --dump-config|grep -i Template
```

Voreingestellt:

```
TemplateDir templates
```

Beispiel:

```
TemplateDir /home/templates
```

Sie können beim Bearbeiten der Vorlagendateien auch andere Schlüsselwörter verwenden.

Es folgt eine Beschreibung der verfügbaren Vorlagen.

HTML-Vorlagen

Vorlage	Bedeutung
alert.html	Wird angezeigt, wenn AntiVir WebGate einen Alarm registriert.
blocked.html	Wird angezeigt, wenn AntiVir WebGate eine verdächtige Datei gesperrt hat (aufgrund der Sperreinstellungen in avwebgate.conf).
error.html	Wird angezeigt, wenn beim Verarbeiten von Benutzeranforderungen ein Fehler auftritt.
progress_downloading.html	Wird beim Herunterladen einer Datei angezeigt. Diese Vorlage findet nur dann Verwendung, wenn die `Refresh`-Methode zum Verhindern von Timeouts eingesetzt wird.
progress_scanning.html	Wird beim Prüfen einer Datei angezeigt. Diese Vorlage findet nur dann Verwendung, wenn die `Refresh`-Methode zum Verhindern von Timeouts eingesetzt wird.
progress_complete.html	Wird angezeigt, nachdem eine Datei heruntergeladen und geprüft wurde. Diese Vorlage findet nur dann Verwendung, wenn die `Refresh`-Methode zum Verhindern von Timeouts eingesetzt wird.
progress_aborted.html	Wird angezeigt, wenn der Benutzer den Download abgebrochen hat. Diese Vorlage findet nur dann Verwendung, wenn die `Refresh`-Methode zum Verhindern von Timeouts eingesetzt wird.
ws_blocked.html	Wird angezeigt, wenn die betreffende Seite einer Kategorie angehört, die vom Benutzer gesperrt wurde.

Email-Vorlagen

Vorlage	Bedeutung
alert.mail	Wird verwendet, wenn AntiVir WebGate einen Alarm registriert.
blocked.mail	Wird verwendet, wenn AntiVir WebGate eine verdächtige Datei gesperrt hat (aufgrund der Sperreinstellungen in avwebgate.conf).

Damit WebGate Email-Nachrichten senden kann, muss ein MTA konfiguriert werden. WebGate kann entweder `mail` *oder* `sendmail` *verwenden. WebGate sucht nach* `/usr/sbin/sendmail`, `/usr/lib/sendmail` *bzw.* `/usr/local/bin/main`, `/bin/mail` *und* `/usr/bin/mail`.

Schlüsselwörter für Vorlagen

Schlüsselwörter werden in %-Zeichen eingeschlossen (z. B. %ALERT%). Nicht alle Schlüsselwörter haben in allen Vorlagen eine Bedeutung. So bleibt beispielsweise das Schlüsselwort ALERT in „progress“-Vorlagen ohne Wirkung.

A = Verfügbar für „alert“-Vorlagen
B = Verfügbar für „blocked“-Vorlagen
E = Verfügbar für „error“-Vorlagen
P = Verfügbar für „progress“-Vorlagen
W = Verfügbar für Webzugriffs- und Inhaltssteuerungsvorlagen von Avira

Schlüsselwort	Beschreibung	Verfügbarkeit
ALERT	Vollständige Alarmmeldung	A
ALERT_DESC	Beschreibung des Alarms	A
ALERT_TYPE	Art des Alarms	A
BLOCKED_REASON	Grund für die Sperrung der Datei	B
CLIENT_IP	IP-Adresse des Clients	A,B
DATA_DIRECTION	„Request“ (Anforderung) oder „response“ (Antwort)	A,B
DATA_PERCENT_RECEIVED	Bereits empfangener Anteil (in Prozent) der Datei, die heruntergeladen wird	P
DATA_RECEIVED	Bereits empfangener Anteil (in Byte) der Datei, die heruntergeladen wird	P
DATA_SIZE	Gesamtgröße (in Byte) der Datei, die heruntergeladen wird	P
DETERMINED_CLIENT_ADDRESS	Adresse des Quell-Clients	A,B
DETERMINED_SERVER_ADDRESS	Adresse des Zielservers	A,B
ENGINE_VERSION	Version von AntiVir Engine	A,B,E
ERROR_CODE	Für die Antwort verwendeter HTTP-Antwortcode	E
ERROR_DESC	Kurzbeschreibung des Fehlers	E
ERROR_REASON	Beschreibung des HTTP-Statuscodes	E

PRODUCT_NAME	„AntiVir WebGate“	A,B,E,P,W
PRODUCT_VERSION	Version von WebGate	A,B,E,P,W
PROGRESS_STATUS	„Downloading“ (Herunterladen), „Scanning“ (Prüfen) usw.	P
PROGRESS_URL	URL zum Abbrechen des Downloads (beim Herunterladen), URL zum Abrufen der Datei (wenn der Vorgang abgeschlossen ist)	P
PROXY_HOST	Hostname des Computers, auf dem WebGate ausgeführt wird	P
QUARANTINE_FILE	Dateiname der in Quarantäne befindlichen Datei	A,B
REFRESH_URL	URL zum Aktualisieren der Fortschrittsseite	P
REQUESTED_FILE	Dateiname der Datei, die heruntergeladen wird	A,B,E,P
REQUESTED_URL	Vollständige URL der Datei, die heruntergeladen wird	A,B,E,P,W
REQUEST_METHOD	„GET“, „POST“ usw.	A,B,E
RESPONSE_STATUS	HTTP-Antwortcode des Servers	A,B,E
MATCHED_CATEGORIES	Alle gesperrten Kategorien, die auf die angeforderte URL zutreffen	W
MATCHED_CATEGORIES_LI	Alle gesperrten Kategorien, die auf die angeforderte URL zutreffen, in Form einer HTML-Liste. Die Listen-Direktiven müssen vom Vorlagen-Designer bereitgestellt werden.	W
SERVER_IP	IP-Adresse des Servers	A,B
VDF_VERSION	Version der AntiVir-VDF-Datei	A,B,E

4.6 Client-Timeout verhindern

WebGate benötigt für die Prüfung immer die vollständige Datei. Die Datei wird deshalb erst geprüft, wenn der Download abgeschlossen ist, und anschließend an den anfordernden Client weitergeleitet. Bei großen Dateien oder einer langsamen Internet-Verbindung kann das Herunterladen längere Zeit in Anspruch nehmen. In diesem Zeitraum erhält der Client keine Rückmeldung. Die Client-Anwendung kann deshalb den Download-Fortschritt nicht anzeigen, und im ungünstigsten Fall kommt es zu Timeout-Problemen.

WebGate stellt verschiedene Methoden bereit, mit denen das Auftreten von Client-Timeouts verhindert werden kann: `refresh`, `redirect` und `keepalive`.

Die Methode zur Timeout-Verhinderung wird dynamisch auf der Grundlage des Client-Typs und/oder der WebGate-Konfigurationseinstellungen ausgewählt. WebGate prüft zunächst, ob die `Refresh`-Methode geeignet ist. Ist dies nicht der Fall, kommt die `Redirect`-Methode zum Einsatz. Funktioniert auch diese Methode nicht, wird die `Keepalive`-Methode verwendet. Ist keine der Methoden geeignet, implementiert WebGate keine Maßnahmen zur Timeout-Verhinderung.

4.6.1 Refresh

Diese Methode kommt bei Clients zum Einsatz, die als Browser identifiziert wurden. WebGate sendet HTML-Seiten mit dem aktuellen Fortschrittsstatus, die in dem mit `RefreshInterval` festgelegten Intervall aktualisiert werden. Nachdem die Datei heruntergeladen und geprüft wurde, kann sie der Benutzer von WebGate abrufen, indem er auf den entsprechenden Link auf der Seite mit der letzten Fortschrittsmeldung klickt. Ist die Datei gesperrt, wird eine HTML-Seite mit einer Warnmeldung aus der entsprechenden Vorlage generiert und an den Client gesendet.

4.6.2 Redirect

Wenn die `Refresh`-Methode nicht verwendet werden kann (weil sie deaktiviert oder der Client kein Browser ist), können stattdessen in einem festgelegten Intervall (`RedirectInterval`) HTTP-`Redirects` an den Client gesendet werden. Der Client wird dadurch zu einer dynamisch generierten URL umgeleitet, die von WebGate identifiziert werden kann und dem entsprechenden Download eindeutig zugeordnet wird. Diese Methode funktioniert jedoch nicht bei jedem Client.

4.6.3 Keepalive

Kann weder die `Refresh`- noch die `Redirect`-Methode verwendet werden (weil sie deaktiviert oder nicht geeignet sind), kommt die `Keepalive`-Methode zum Einsatz.

Bei dieser Methode sendet WebGate in einem festgelegten Intervall (`KeepaliveInterval`) erweiterte Header-Daten (X-WebGate-Status) an den Client. Diese werden vom Client nicht interpretiert, reichen aber oft aus, um den Timeout zurückzusetzen. Wenn sich zwischen WebGate und den Clients ein

Proxyserver befindet, funktioniert diese Timeout-Methode möglicherweise nicht.

Data-Trickling

Wenn die oben beschriebenen Verfahren zur Verhinderung von Timeouts in Ihrer Umgebung nicht umgesetzt werden können oder nicht funktionieren und deshalb Client-Timeouts auftreten, können Sie das Data-Trickling aktivieren, indem Sie in avwebgate.conf die Option `KeepaliveMode` auf „trickle“ setzen. WebGate sendet die Daten dann in kleinen Paketen in dem mit `KeepaliveInterval` festgelegten Intervall, bis Download und Überprüfung abgeschlossen sind. Nachdem die Datei heruntergeladen und überprüft wurde, wird sie sehr schnell an den Client weitergeleitet (sofern sie keine infizierten Daten enthält).

Das Data-Trickling funktioniert zwar in der Regel in jeder Umgebung und bei jedem Client, stellt aber keine optimale Lösung dar. Folgende Punkte müssen beachtet werden, wenn Data-Trickling eingesetzt werden soll:

- An den Client werden bereits kleine Datenpakete gesendet, bevor die Datei vollständig heruntergeladen und geprüft ist. Es besteht deshalb ein gewisses Risiko, dass die per Data-Trickling gesendeten Daten einen Virus enthalten. Dieses Risiko ist sehr gering, darf aber nicht ignoriert werden. WebGate beginnt zwar bereits vor dem Start des Data-Tricklings mit der Prüfung der Daten, die von der Datei bereits empfangen wurden, das Prüfergebnis ist aber möglicherweise nicht korrekt, da die Datei zum Zeitpunkt der Prüfung nicht vollständig vorlag.
- Die auf dem Client angezeigte Download-Geschwindigkeit entspricht der Geschwindigkeit, mit der der Client die per Trickling übertragenen Daten empfängt. Sie entspricht nicht der tatsächlichen Geschwindigkeit, mit der WebGate die Datei empfängt.
- Die vom Client berechnete Übertragungszeit ist unzutreffend und viel zu lang.
- Wenn ein Virus erkannt wird, nachdem der erste Teil der Datei bereits per Data-Trickling übertragen wurde, kann an den Client keine Benachrichtigung (z. B. eine HTML-Seite mit einer Warnung) gesendet werden. WebGate beendet in diesem Fall lediglich die Verbindung zum Client. Unter Umständen bleiben dann kleine, unvollständige (normalerweise unbrauchbare) Dateien auf dem Client zurück, die vom Benutzer gelöscht werden müssen.

Das Data-Trickling sollte nur verwendet werden, wenn die anderen Methoden zur Verhinderung von Timeouts nicht zum Erfolg führen. Beachten Sie die Risiken und Einschränkungen dieses Verfahrens, bevor Sie diese Funktion aktivieren.

4.7 Erweiterte Optionen

Mit den folgenden Optionen kann eine Feinabstimmung von WebGate vorgenommen werden. Eine Änderung dieser Einstellungen ist normalerweise nicht erforderlich. In Spezialfällen und in bestimmten Umgebungen kann eine Anpassung jedoch sinnvoll sein:

4.7.1 Proxy-Einstellungen

DNSHelpers **DNSHelpers**

Wertebereich: Minimum 0, Maximum 64

Beispiel:

```
DNSHelpers 10
```

Voreingestellt:

```
DNSHelpers 8
```

Die Anzahl der DNS-Hilfsprozesse, die beim Start erstellt werden. Diese Option ermöglicht gleichzeitige DNS-Lookups, sodass sich die Ausführungsgeschwindigkeit erhöht. Der zulässige Höchstwert ist 64.

ClientTimeout **ClientTimeout**

Wertebereich: Minimum 0, Maximum 600

Beispiel:

```
ClientTimeout 120
```

Voreingestellt:

```
ClientTimeout 60
```

Die Zeit in Sekunden, die auf eine Anforderung des Clients gewartet wird. Nach Ablauf dieser Zeit tritt ein Timeout auf und die Sitzung wird beendet.

ServerTimeout **ServerTimeout**

Wertebereich: Minimum 0, Maximum 600

Beispiel:

```
ServerTimeout 240
```

Voreingestellt:

```
ServerTimeout 120
```

Die Zeit in Sekunden, die auf eine Anforderung des Servers gewartet wird. Nach Ablauf dieser Zeit tritt ein Timeout auf und die Sitzung wird beendet.

OpenMax **OpenMax**

Wertebereich: Minimum 0, Maximum 2147483647

Beispiel:

```
OpenMax 1000
```

Voreingestellt:

```
OpenMax 0
```

Diese Option legt die maximale Anzahl geöffneter Dateien für den WebGate-Prozess fest. Mit der Voreinstellung `0` wird WebGate keine der bestehenden Systemwerte verändern.

WorkerPoolSize

WorkerPoolSize

Wertebereich: Minimum 0, Maximum 20000

Beispiel:

```
WorkerPoolSize 100
```

Voreingestellt:

```
WorkerPoolSize 0
```

Die Anzahl der Threads im Thread-Pool. Bei der Einstellung 0 ist der Thread-Pool deaktiviert, sodass für jede Anforderung ein neuer Thread erzeugt wird. Sie aktivieren diese Option, indem Sie einen Wert größer `0` angeben.

ScannerPool Size

ScannerPoolSize

Wertebereich: Minimum 0, Maximum 250

Beispiel:

```
ScannerPoolSize 70
```

Voreingestellt:

```
ScannerPoolSize 100
```

Die Anzahl der persistenten Verbindungen zum Scanner. Bei der Einstellung 0 ist der Pool für persistente Verbindungen deaktiviert, sodass für jede Anforderung eine neue Verbindung zum Scanner aufgebaut wird. Im Pool für persistente Verbindungen wird eine bestimmte Anzahl offener Verbindungen zum Scanner verwaltet, sodass nicht für jede Anforderung eine Verbindung aufgebaut und wieder beendet werden muss. Der Prüfvorgang kann dadurch schneller ausgeführt werden.

Diese Option ist eng mit der Option `PoolScanners` in avwebgate-scanner.conf verknüpft, die festlegt, wie viele Verbindungen die Scanner akzeptieren.

WebGate versucht, die festgelegte Anzahl von Verbindungen aufzubauen.

Wenn für `PoolScanners` ein kleinerer Wert festgelegt ist oder nicht alle Scanner-Verbindungen verfügbar sind (weil einige von einem anderen Prozess genutzt werden), erstellt WebGate die größtmögliche Anzahl von Verbindungen.

4.7.2 Datenbankunterstützung

WebGate unterstützt die Protokollierung von statistischen Informationen in einer Datenbank. Einzelheiten zur Einrichtung der Datenbank und zu anderen Anforderungen finden Sie unter Anforderungen an die Datenbankkonfiguration.

Die Datenbank enthält zwei Tabellen mit den Namen `alerts` (Warnmeldungen) und `counter` (Statistiken).
`Alerts` enthält Informationen über Warnmeldungen, die von WebGate empfangen wurden. Abhängig von den Einstellungen des Parameters `LogCleanRequests`, kann die Tabelle `alerts` auch alle Anforderungen die von WebGate bearbeitet wurden, anzeigen.

`Counter` enthält WebGate-spezifische Statistiken für Nachschlagezwecke.

Protokollierung in „alerts“

- status (Prüf-Flags; durch ACL gesperrt; Filter, der die Anforderung gesperrt hat; unverdächtig und getunnelt, falls zutreffend)
- url
- alert_url
- alertname
- action (gesperrt, zulässig, getunnelt, in Quarantäne, gelöscht)
- source
- category (empfangen von WebProtector, WebCat und RTSP)
- engine
- date
- vdf

Protokollierung in „counter“

- Anzahl der Dateien, die aufgrund der Namenserweiterung gesperrt wurden
- Anzahl der Dateien, die aufgrund verdächtigen Verhaltens gesperrt wurden: Fehler bei der Verarbeitung, teilweise vorhandene, nicht unterstützte, verschlüsselte Archive, erreichte Grenzwerte (maximale Größe, maximale Rekursionstiefe usw.)
- Anzahl der infizierten Dateien
- Anzahl der unverdächtigen Dateien
- Anzahl der geprüften Dateien
- Gesamte empfangene Datenmenge in Byte

Optionen

DBSupport

DBSupport

Wenn diese Option aktiviert ist, protokolliert WebGate statistische Daten in einer Datenbank. Die Datenbank besteht aus zwei Tabellen: `alerts` und `counter`. Um die Datenbankunterstützung einzurichten, müssen Sie den `GUISupport` aktivieren. Achten Sie darauf, dass die GUI... Zertifikatsdateien entsprechend konfiguriert sind.

Syntax:

```
DBSupport "YES|NO"
```

Voreingestellt:

```
DBSupport NO
```

DBodbcIni

DBodbcIni

Wenn die Option `DBSupport` aktiviert ist, verwendet der ODBC-Treibermanager die angegebene odbc.ini-Datei. Standardeinstellung: Der installierte ODBC-Treibermanager entscheidet, welche odbc.ini-Datei geladen wird.

Syntax:

```
DBodbcIni "string"
```

Beispiel:

```
DBodbcIni /Pfad/zu/odbc.ini
DBodbcIni /etc/avira/avwebgate-odbc.ini
```

DBodbcLib

DBodbcLib

Wenn die Option `DBSupport` aktiviert ist, lädt WebGate die angegebene Bibliothek und verwendet sie als ODBC-Treibermanager. Standardeinstellung: WebGate sucht im Standardbibliothekspfad (in der angegebenen Reihenfolge) nach folgenden Dateien und lädt eine dieser Dateien: libodbc.so.1, libodbc.so, libiodbc.so.

Syntax:

```
DBodbcLib "string"
```

Beispiel:

```
DBodbcLib /Pfad/zu/odbc-library
```

DBodbcData Source

DBodbcDataSource

Wenn die Option `DBSupport` aktiviert ist, wird die angegebene Datenbank als Quelle verwendet.

Syntax:

```
DBodbcDataSource "string"
```

Voreingestellt:

```
DBodbcDataSource WebGate
```

DBUpdate Delay

DBUpdateDelay

Wenn die Option `DBSupport` aktiviert ist, werden die statistischen Daten in regelmäßigen Abständen in der Datenbank aufgezeichnet. Das Intervall kann in Sekunden (s), Minuten (m) oder Stunden (h) angegeben werden. Wenn Sie den Wert auf `0` setzen, wird das voreingestellt Zeitinterval von 1 Stunde verwendet. Standardeinstellung: eine Stunde.

Syntax:

```
DBUpdateDelay "timespan"
```

Voreingestellt:

```
DBUpdateDelay 1h
```

DBLogClean Requests

DBLogCleanRequests

Wenn die Option `DBSupport` aktiviert ist, werden Anforderungen, die WebGate als unverdächtig einstuft, standardmäßig nicht zur Datenbank hinzugefügt. Mit dieser Option kann die Standardeinstellung geändert werden.

Syntax:

```
DBLogCleanRequests "YES|NO"
```

Beispiel:

```
DBLogCleanRequests YES
```

Voreingestellt:

```
DBLogCleanRequests NO
```

Anforderungen an die Datenbankkonfiguration

Es folgt eine Liste mit Versionsnummern von kompatiblen MySQL-Servern, MySQL-ODBC-Treibern und ODBC-Treibermanagern:

MySQL 5.0.70
MySQL-ODBC-Treiber 3.51.11
iODBC 3.52.4

Einrichtung

Bevor Sie die Datenbankunterstützung aktivieren, müssen Sie einen ODBC-Treibermanager installieren und einrichten. Es sind zwei Treibermanager verfügbar:

iODBC – www.iodbc.org (empfohlen)
unixODBC – www.unixodbc.org

Unten finden Sie eine Beschreibung, wie Sie ODBC unter Debian 5.0 installieren und einrichten können. (Informationen über die Installation und Einrichtung von ODBC bei Verwendung eines anderen Betriebssystems finden Sie im Distributions- bzw. im Managerhandbuch.)

Warnung: *Bei WebGate handelt es sich um ein 32-Bit-Binärprogramm, das keine gemeinsamen 64-Bit-Objekte verwenden kann. Das bedeutet, dass die Verwendung eines 64-Bit-ODBC-Treibermanagers nicht möglich ist.*

Auf 64-Bit-Computern sollten Sie darauf achten, dass es sich bei der ODBC-Verbindung um ein gemeinsames 32-Bit-Objekt handelt. Einzelheiten zur Einrichtung der Datenbankunterstützung in WebGate auf einem 64-Bit-Computer finden Sie in der Datei README.db-support-SLES10-SP2-64bit.

Diese Datei enthält eine Beispieleinrichtung für ODBC unter SuSE Linux Enterprise 10 SP2.

1. Datenbank einrichten

Wenn Sie noch keinen Benutzer mit Zugriffsrechten auf die Datenbank eingerichtet haben, sollten Sie jetzt einen einrichten.
Informationen darüber, wie Sie einen Benutzer zu Ihrer Datenbank hinzufügen und diesem Zugriff geben können, finden Sie im Handbuch zu Ihrer Datenbank.

Einzelheiten zum Datenbanklayout finden Sie in der Datei /usr/lib/AntiVir/webgate/create-db.sql. Das Datenbanklayout ist das Skript zur Erstellung einer MySQL-Datenbank.

Sie können die Datenbank mit diesem Skript erstellen (Beispiel für MySQL, wobei der Server auf dem angegebenen Host ausgeführt wird):

```
# mysql -u <db-Benutzer> -p -h <Name Ihres SQL-Server-
Hosts> < create-db.sql
```

Geben Sie das Passwort ein.

2. iODBC installieren

Sie sollten eine threadsichere Bibliothek wählen. Überprüfen Sie anhand des Handbuchs der Distribution, ob Ihre ODBC-Bibliothek mit Threadunterstützung eingerichtet wurde.

```
# apt-get install libiodbc2
```

3. Datenbanktreiber für die Datenbank installieren

Sie sollten einen threadsicheren Treiber wählen. Überprüfen Sie anhand des Handbuchs der Distribution, ob Ihr ODBC-Treiber threadsicher ist.

Beispiel für MySQL-ODBC-Treiber:

```
# apt-get install libmyodbc
```

4. odbc.ini einrichten (unter 5. ist ein Beispiel für odbc.ini aufgeführt)

Zur Einrichtung gibt es verschiedene Möglichkeiten:

- Erstellen und/oder bearbeiten Sie /etc/odbc.ini.
  oder
- Kopieren Sie /etc/avira/avwebgate-odbc.ini in /etc/odbc.ini und bearbeiten Sie die Datei.
  oder
- Bearbeiten Sie /etc/avira/avwebgate-odbc.ini, und setzen Sie die Konfigurationsoption „`DBodbcIni`“ in /etc/avira/avwebgate.conf auf „/etc/avira/avwebgate-odbc.ini“.

Wenn Sie den Pfad odbc.ini aus dem Avira Security Management Center heraus konfigurieren möchten, beachten Sie bitte, dass dies nicht über die SMC GUI möglich ist. Sie können den Pfad manuell zum Clientrechner kopieren, zum Beispiel mit Hilfe von SCP oder WinSCP, oder Sie verwenden die Kopierfunktion für Dateien im SMC. Vergewissern Sie sich, dass die Dateien nicht schreibgeschützt sind. Sie können das Schreibrecht manuell über SSH erteilen oder die `chmod`-Hilfskonstruktion verwenden: /bin/chmod a+w/usr/lib/AntiVir/agent/webgate-odbc.ini.

Wenn Sie die Datenbankunterstützung durch Editieren der Datei avwebgate-odbc.ini *konfigurieren, achten Sie bitte genauestens auf die Richtigkeit Ihrer Einträge. Eventuelle Leerzeichen vor dem Optionsnamen führen zu Fehlermeldungen.*

Wenn Sie „`DBodbcIni`*“ in* /etc/avira/avwebgate.conf *nicht angeben, entscheidet die Bibliothek, wo nach* odbc.ini *gesucht wird.*

Die Bibliothek verwendet möglicherweise auch eine andere odbc.ini*-Datei, wenn die angegebene Datei vorhanden, aber durch den Benutzer, in dessen Namen WebGate ausgeführt wird, nicht lesbar bzw. beschreibbar ist.*

5. Beispiel für odbc.ini

Dies ist ein Beispiel für eine minimale odbc.ini-Datei.

Details zu den verfügbaren Optionen finden Sie in der Dokumentation zu Ihrem Datenbanktreiber.

[WebGate]
Driver = /usr/lib/odbc/libmyodbc.so
Server = hostname.of.my.sql.server
User = username
Password = password
Database = webgate

[WebGate]: Der von WebGate verwendete DSN
Driver: Der Pfad zur Bibliothek des Treibers
Server: Der Datenbankserver
User: Der Benutzername für den Zugriff auf die DatenbankPassword:Das zum Benutzernamen gehörige Passwort
Database: Der Name der zu verwendenden Datenbank

6. Datenbankunterstützung in avwebgate.conf aktivieren

Setzen Sie „DBSupport“ in /etc/avira/avwebgate.conf auf YES.

7. ODBC-Einrichtung testen

Sie können die Datenbankkonnektivität mit dem Tool `avwg_stats` prüfen. Das Tool wird durch WebGate gestartet, wenn `DBSupport` und `GuiSupport` aktiviert sind. Zunächst analysiert `avwg_stats` die Konfigurationsdatei nach Validität. Das Tool wird für die Kommunikation zwischen Datenbank und Client, Datenbank und SMC sowie für Datenbankprotokolleinträge verwendet.

```
/usr/lib/AntiVir/webgate/gui/bin/avwg_stats -S
```

Das Tool gibt bei Erfolg Folgendes aus:

```
$ /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -S
Using these settings:
ODBC ini:    <using system's odbc.ini.>
ODBC library: libodbc.so.1
ODBC source: WebGate

Preparing connection ...
=> OK
Connecting ...
=> OK
Disconnecting ...
=> OK

Successfully verified database connectivity!
```

... und beim Auftreten von Fehlern eine ähnliche Liste (Beispiel für MySQL; die Fehlermeldung kann sich je nach Fehlertyp unterscheiden):

```
Using these settings:
ODBC ini:    <using system's odbc.ini.>
ODBC library: libodbc.so.1
ODBC source: WebGate

Preparing connection ...
=> OK
Connecting ...
Failed to connect to ODBC data source (error code: -2)
([MySQL][ODBC 3.51 Driver]Lost connection to MySQL server at 'reading
initial communication packet', system error: 111)
```

Ausgabe einer CSV-Liste

WebGate kann die Tabelleninhalte als CSV-Liste (durch Komma getrennte Werte) ausgeben.
Standardmäßig wird nur die Tabelle `alerts` ausgegeben. Sie können mit der Befehlszeilenoption `-t` auch eine andere Tabelle ausgeben lassen.

Die erste Zeile der ausgegebenen Liste enthält die Spaltennamen. Alle anderen Zeilen bilden die Tabellenzeilen. Die Ergebnisse sind nicht sortiert.

Beispiel:

Ausgabe der Tabelle `alerts`:

```
# /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -o csv
```

Ausgabe der Tabelle `counter:`

```
# /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -o csv -
t counter
```

CSV-Trennzeichen:

Geben Sie ein einzelnes Feldtrennzeichen an:

```
-o csv:"s"
```

Sie müssen das Trennzeichen in Anführungszeichen angeben, da es andernfalls eventuell von der Shell interpretiert wird.

Beispiel:

Ausgabe der Tabelle `alerts` mit ";" als Trennzeichen:

```
# /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -o
csv:";"
```

Zeitabschnitte:

Sie können das Ergebnis auf die Auflistung von Zeilen innerhalb eines bestimmten Zeitabschnitts beschränken:

```
-R "YYYY-MM-DD HH:MM:SS/YYYY-MM-DD HH:MM:SS"
```

Beispiel:

Ausgabe der Tabelle `alerts` unter Beschränkung auf einen bestimmten Zeitabschnitt:

```
# /usr/lib/AntiVir/webgate/gui/bin/avwg_stats -o csv -
R "2011-04-13 00:00:00/2011-04-13 15:35:43"
```

Hierdurch werden alle Warnmeldungen aufgelistet, die zwischen 2011-04-13 00:00:00 und 2011-04-13 15:35:43 protokolliert wurden.

Beschreibung der Tabelle `alerts`

Sobald eine Email blockiert wird, werden Angaben zur Warnmeldung/zu den Warnmeldungen in die Datenbank geschrieben.

Spalte	Beschreibung
id	Diese Spalte beinhaltet eine automatisch generierte aufsteigende Zahl.
reason	Der Grund, warum die Anfrage blockiert wurde. Es gibt folgende Gründe: *Alert* - Der Scanner hat Malware gefunden. *Suspicious* - Der Scanner hat eine verdächtige Datei entdeckt *Error* - Fehler beim Scannen *Incomplete* - nicht vollständig gescannt *Encrypted* - Der Scanner hat eine verschlüsselte Datei gefunden *Extension* - Die Dateierweiterung wurde blockiert *Archive bomb* - Der Scanner hat eine Archivbombe gefunden *ACL* - Anforderung wurde durch Zugriffssteuerungsregeln (ACL) blockiert *Online filter* - Anforderung wurde durch den Online Filter blockiert *Local filter* - Anforderung wurde durch den lokalen Filter blockiert *RTPS filter* - Anforderung wurde durch den RTPS-Filter blockiert *Clean* - Anforderung wurde zugelassen *Tunneled* - Anforderung wurde getunnelt (nicht gescannt) *Unsupported* - Der Scanner hat ein nichtunterstütztes Archiv gefunden ***Hinweis**: Nach Produktaktualisierungen werden in dieser Spalte zukünftig möglicherweise noch andere Gründe aufgeführt.*

Spalte	Beschreibung
alertname	vom Grund abhängig: *Alert* - die Bezeichnung der Warnmeldung *All other reasons* - eine detaillierte Beschreibung des Grundes
alerttype	Zusätzliche Informationen über die Warnmeldung: *Alert* -adware, backdoor, trash, dialer, heuristic, joke, program, riskware, trojan, virus, worm (***Hinweis**: In dieser Spalte werden möglicherweise auch andere Kategorien verwendet. Die Kategorien hängen vom Scanner ab und können sich ändern, oder es stehen nach einer Aktualisierung des Scanners möglicherweise neue zur Verfügung.)* *All other reasons* - eine kurze Beschreibung der Bezeichnung der Warnmeldung
filename	Die vollständige URL der Datei, die heruntergeladen wird.
action	Die ausgeführte Aktion: gelöscht, in Quarantäne, zulässig, blockiert, getunnelt
source	Die IP des Client, der die Anforderung gestellt hat
category	Wenn die Option `BlockCategories` aktiviert ist, werden die von `WebProtector`, `RTPS` und `UrlCheck` zurückgegebenen Kategorien hier geschrieben.
alerturl	Eine URL mit mehr Informationen über die Warnmeldung (wenn es eine Warnung gab). So wird zum Beispiel für das Testprogramm Eicar folgende URL hinzugefügt: http://www.avira.com/en/threats?q=Eicar%2DTest%2DSignature
missed	Aufgrund interner Pufferbeschränkungen kann möglicherweise nicht jede Warnmeldung in die Datenbank geschrieben werden. In diesem Fall enthält die Spalte "missed" eine Angabe zur Anzahl der Warnmeldungen, die nicht in die Datenbank geschrieben werden konnten.
product	Enthält den Produktnamen "WebGate".
vdf	Versionsinformationen zu der zum Scannen verwendeten VDF.
engine	Versionsinformationen zu der zum Scannen verwendeten Engine.

Spalte	Beschreibung
hostname	Der Wert von "MyHostName" (/etc/avira/avwebgate.conf) Wenn "MyHostName" nicht festgelegt ist, ist dies der von `gethostname`() zurückgegebene Wert; wenn `gethostname`() fehlschlägt, "localhost".
ou	Wenn `ActiveDirectorySupport` aktiviert und ein Lookup für eine Gruppe durchgeführt wurde, wird der gefundene Wert in diese Spalte zurückgeschrieben.

Beschreibung der Tabelle `counter`

Die Spalten in der Tabelle "counter" werden regelmäßig ausgefüllt. Die Standardeinstellung ist zu jeder vollen Stunde.

Sie können den Zeitraum zwischen den Einträgen über die Konfigurationsoption `DBUpdateDelay` in /etc/avira/avwebgate.conf ändern.

Beispiel:

```
DBUpdateDelay 30m
```

Informationen werden alle 30 Minuten in die Datenbank geschrieben.
Mögliche Einheiten sind: keine Einheit/s=Sekunden, m=Minuten, h=Stunden

Spalte	Beschreibung
id	Diese Spalte beinhaltet eine automatisch generierte aufsteigende Zahl.
accepted	Die Gesamtzahl der gescannten Dateien.
clean	Die Anzahl der unverdächtigen Dateien.
alerts	Die Anzahl der gefundenen Malware.
acl	Die Anzahl der Dateien, die durch ACLs blockiert wurden.
total_size	Das Gesamtaufkommen des Datenverkehrs.
errors	Die Anzahl der Anforderungen, die bei der Verarbeitung einen Fehler verursacht haben.
incomplete	Die Anzahl der Anforderungen, die nicht vollständig gescannt werden konnten.
unsupported	Die Anzahl der Anforderungen mit einem nicht unterstützten Komprimierungsverfahren.
encrypted	Die Anzahl der Anforderungen mit verschlüsselten Anhängen.
extension	Die Anzahl der Dateien, deren Anhang eine verbotene Dateierweiterung enthält.

Spalte	Beschreibung
limits	Die Anzahl der Dateien, bei deren Verarbeitung ein Archivgrenzwert erreicht wurde.
url_filter	Die Anzahl der Dateien, die durch die URL Filter (`RTPS`, `WebCat`, `WebProtector`) blockiert wurden.
product	Der Produktname "WebGate".
hostname	Der Wert von "MyHostName" (/etc/avira/avwebgate.conf). Wenn "MyHostName" nicht festgelegt ist, ist dies der von `gethostname`() zurückgegebene Wert. Wenn `gethostname`() fehlschlägt, "localhost".

Getunnelte Verbindungen werden in der Tabelle `counter` *nicht gelistet.*

4.7.3 Einstellungen der HTTP-Verbindung

AllowHTTP Connect

AllowHTTPConnect

Syntax:

```
AllowHTTPConnect "YES|NO"
```

Voreingestellt:

```
AllowHTTPConnect NO
```

Mit dieser Option können Sie es WebGate ermöglichen, eine Tunnelverbindung zu einem beliebigen für HTTP zulässigen Port herzustellen, wenn eine Anforderung für eine CONNECT-Methode empfangen wird.

Verwenden Sie diese Option mit Vorsicht. Die über die Tunnelverbindung übertragenen Daten werden von WebGate nicht geprüft. Wenn Sie nur Verbindungen zu den Ports 443 (HTTPS) und 563 (SNEWS) zulassen möchten, verwenden Sie die Option `AllowHTTPSTunnel`.

ProgressAuto Send

ProgressAutoSend

Syntax:

```
ProgressAutoSend "YES|NO"
```

Voreingestellt:

```
ProgressAutoSend NO
```

Mit dieser Option können Sie veranlassen, dass die Datei automatisch an den Client gesendet wird, nachdem der Download-Fortschritt angezeigt (bei der Aktualisierung der HTML-Seiten) und der Download abgeschlossen wurde (funktioniert möglicherweise nicht bei allen Clients).

Progress Filesize Threshold

ProgressFilesizeThreshold

Beispiel:

```
ProgressFilesizeThreshold 1K
```

Voreingestellt:

```
ProgressFilesizeThreshold 20MB
```

Wenn Dateien heruntergeladen werden, die größer sind als hier angegeben, werden unabhängig von der Art des Inhalts und der Namenserweiterung Fortschrittsmeldungen an den Client gesendet. Der Wert 0 bedeutet, dass die Dateigröße bei der Auswahl der Methode zur Timeout-Verhinderung nicht berücksichtigt wird.

ProgressHold Time

ProgressHoldTime

Wertebereich: Minimum 0, Maximum 36000

Beispiel:

```
ProgressHoldTime 2400
```

Voreingestellt:

```
ProgressHoldTime 1800
```

Die Zeit (in Sekunden), die auf eine `Refresh`- oder `Redirect`-Anforderung des Clients gewartet wird, nachdem der Download-Fortschritt angezeigt und der Download-Vorgang abgeschlossen wurde. Geht innerhalb dieses Zeitraums keine Anforderung ein, wird die Datei verworfen.

ProgressHold TimeAfter GetFile

ProgressHoldTimeAfterGetFile

Wertebereich: Minimum 0, Maximum 7200

Beispiel:

```
ProgressHoldTimeAfterGetFile 1200
```

Voreingestellt:

```
ProgressHoldTimeAfterGetFile 0
```

Die Zeit (in Sekunden), die auf weitere Anforderungen des Clients gewartet wird, nachdem dieser die heruntergeladene Datei mindestens einmal über den Link zum Abrufen der Datei auf der letzten Fortschrittsseite von WebGate angefordert hat. Der Client hat so die Möglichkeit, die zwischengespeicherte Datei mehrmals abzurufen. Geht innerhalb des festgelegten Zeitraums keine Anforderung ein, wird die Datei gelöscht. Standardmäßig werden Dateien sofort gelöscht, nachdem sie einmal an den Client gesendet wurden.
Für Squid (Version < 2.5.STABLE9) sollte diese Option auf einen Wert größer 0 eingestellt werden. Squid wiederholt die Anforderung nämlich dreimal, wenn die Antwort 403 übermittelt wurde, während WebGate die angeforderte Seite bereits nach der ersten Anforderung löscht.

ProgressHost

ProgressHost

Beispiel:

```
ProgressHost home.security:port
```

Voreingestellt:

```
ProgressHost Avira.WebGate:80
```

Der Hostname für die Fortschritts-URL. Sie können einen „echten“ Namen bzw. eine „echte“ Adresse angeben, wenn beispielsweise Probleme mit DNS-Lookups des Browsers oder des Proxyservers auftreten. Der Port muss angegeben sein.

RefreshDelay

RefreshDelay

Wertebereich: Minimum 0, Maximum 600

Beispiel:

```
RefreshDelay 60
```

Voreingestellt:

```
RefreshDelay 3
```

Mit dieser Option wird die Wartezeit (in Sekunden) vor dem erstmaligen Senden der Fortschrittsmeldung an den Client festgelegt. Bei Seiten, die langsam geladen werden, können Sie so verhindern, dass WebGate den Aktualisierungsbildschirm anzeigt. Wenn der Wert dieser Option niedriger ist als der von `RefreshInterval`, wird die `RefreshInterval`-Einstellung wirksam.

RefreshSkipFile Extensions

RefreshSkipFileExtensions

Beispiel:

```
RefreshSkipFileExtensions xml, htm
```

Voreingestellt:

```
RefreshSkipFileExtensions htm, html, shtml, css, gif,
jpg, jpeg, png, swf, flv
```

Mit dieser Option wird das Senden von Aktualisierungsmeldungen verhindert, wenn große Dateien mit den angegebenen Erweiterungen heruntergeladen werden.

Refresh Timeout

RefreshTimeout

Wertebereich: Minimum 0, Maximum 3600

Beispiel:

```
RefreshTimeout 60
```

Voreingestellt:

```
RefreshTimeout 30
```

Wenn innerhalb des (in Sekunden angegebenen) Timeout-Intervalls (plus der Zeit für die `Refresh`-/`Redirect`-Aktion) keine `Refresh`- oder `Redirect`-Anforderung eingeht, wird der Download automatisch abgebrochen.

CheckHTTPS Handshake

CheckHTTPSHandshake

Syntax:

```
CheckHTTPSHandshake "YES|NO"
```

Voreingestellt:

```
CheckHTTPSHandshake YES
```

WebGate prüft standardmäßig, ob auf eine CONNECT-Anforderung ein HTTPS-Handshake folgt. Wenn dieses Verhalten nicht erwünscht ist, setzen Sie `CheckHTTPSHandshake` auf NO.

UseActiveFTP

UseActiveFTP

Syntax:

```
UseActiveFTP "YES|NO"
```

Voreingestellt:

```
UseActiveFTP NO
```

Bei Verwendung von „FTP über HTTP“ wird die FTP-Verbindung zwischen WebGate und FTP-Server im passiven Modus hergestellt. Wenn dies nicht erwünscht ist, können Sie veranlassen, dass der aktive Modus verwendet wird, indem Sie `UseActiveFTP` auf 1 einstellen. Diese Option hat nur eine Wirkung, wenn „FTP über HTTP“ verwendet wird (die Dateien auf einem FTP-Server also mit einem Browser angezeigt werden). Wird WebGate als FTP-Proxy eingesetzt, stellt der verwendete FTP-Client den aktiven oder passiven Modus ein.

AllowActive FTPPorts

AllowActiveFTPPorts

Beispiel:

```
AllowActiveFTPPorts 33323
```

Voreingestellt:

```
AllowActiveFTPPorts 0
```

Bei der Herstellung aktiver FTP-Verbindungen im Modus „FTP über HTTP“ wird der Port, über den der Server kommuniziert, normalerweise nach dem Zufallsprinzip ausgewählt. WebGate bietet alternativ die Möglichkeit, eine Liste der Ports zu definieren, über die kommuniziert werden soll. Sie können einen oder mehrere Einzelports angeben (z. B. 15673 60754) oder Portbereiche definieren. Zur Angabe eines Bereichs verbinden Sie die betreffenden Portnummern mit einem Minuszeichen (-). Beispiel: 1025-65535. Vor und nach dem Minuszeichen darf kein Leerzeichen eingefügt werden.

Wenn die Liste Portnummern unter 1024 enthält, müssen Sie WebGate als root ausführen, indem Sie User und Group in avwebgate.conf *auf „root“ setzen. Da dies jedoch ein Sicherheitsrisiko darstellt, sollte dieses Vorgehen vermieden werden.*

4.7.4 Einstellungen der FTP-Verbindung

FTPDefault Server

FTPDefaultServer

Beispiel:

```
FTPDefaultServer ftp.example.com:21
```

Voreingestellt:

```
NONE
```

Mit dieser Option kann der FTP-Server festgelegt werden, zu dem WebGate standardmäßig eine Verbindung aufbaut, wenn das Programm als FTP-Proxy ausgeführt wird. Auf diese Weise lässt sich beispielsweise ein einzelner FTP-Server „transparent“ schützen.

FTPProxy Username

FTPProxy Benutzername

Beispiel:

```
FTPProxyUsername benutzer@beispiel
```

Voreingestellt:

```
NONE
```

FTPProxy Password

FTPProxy Passwort

Beispiel:

```
FTPProxyPassword password
```

Voreingestellt:

```
NONE
```

Die Optionen `FTPProxyUsername` und `FTPProxyPassword` werden gesetzt, wenn WebGate einen FTP-Parent-Proxyserver verwendet.

4.7.5 Einstellungen der ICAP-Verbindung

ICAPError ResponseOn Blocked

ICAPErrorResponseOnBlocked

Syntax:

```
ICAPErrorResponseOnBlocked "YES|NO"
```

Voreingestellt:

```
ICAPErrorResponseOnBlocked NO
```

Mit dieser Option kann die ICAP-Antwort geändert werden, die für eine gesperrte Datei an den ICAP-Client gesendet wird. Standardmäßig sendet WebGate die ICAP-Antwort 200 mit dem HTTP-Fehler 403 sowie eine HTML-Seite, die aus der entsprechenden HTML-Vorlage erzeugt wird. Wenn diese Option aktiviert ist, sendet WebGate stattdessen die ICAP-Antwort 403 (ohne Meldungstext) an den ICAP-Client.

4.7.6 Einstellungen zum Verhindern von Timeouts

In Abhängigkeit zur Art des Clients und zu den Konfigurationseinstellungen von WebGate wird die Methode zum Verhindern von Timeouts dynamisch entschieden. Alle Einstellungen legen fest, in welchem Zeitintervall die Methode wiederholend arbeitet. Gültige Zeitfaktoren sind:

- `s` für Sekunden (voreingestellt ist, dass ein Wert ohne weitere Angaben als Sekunden gelesen wird)
- `m` für Minuten
- `h` für Stunden

KeepaliveDelay

KeepaliveDelay

Wertebereich: Minimum 0, Maximum 600

Beispiel:

```
KeepaliveDelay 60
```

Voreingestellt:

```
KeepaliveDelay 0
```

Diese Option ist nur wirksam, wenn `KeepaliveMode` auf `trickle` eingestellt ist. Diese Funktion birgt Sicherheitsrisiken, die minimiert werden können, indem `KeepaliveInterval` nicht auf einen Wert <30 eingestellt wird. Es gibt jedoch Situationen, bei denen die ersten Bytes bereits kurz nach dem Start des Downloads empfangen werden sollen (um z. B. das Dialogfeld „Speichern unter“ anzuzeigen). Mit dieser Option wird die Wartezeit (in Sekunden) vor dem Start des Data-Tricklings festgelegt.

KeepaliveMode

KeepaliveMode

Syntax:

```
KeepaliveMode "trickle|header"
```

Voreingestellt:

```
KeepaliveMode header
```

Um Client-Timeouts beim Herunterladen und Prüfen großer Dateien zu vermeiden, sendet WebGate in dem mit `KeepaliveInterval` festgelegten Intervall erweiterte Header-Daten (X-WebGate-Status) an den Client. Durch Einstellen dieser Option auf `trickle` kann das Data-Trickling aktiviert werden. WebGate sendet dann kleine Datenpakete der Datei an den Client, bis die gesamte Datei heruntergeladen und geprüft ist.

Verwenden Sie diese Option mit Vorsicht. Theoretisch besteht die Möglichkeit, dass Viren übertragen werden. Beachten Sie die Risiken und Einschränkungen dieses Verfahrens, bevor Sie das Data-Trickling aktivieren (siehe 4.6 Client-Timeout verhindern).

TrickleDataSize

TrickleDataSize

Beispiel:

```
TrickleDataSize 2
```

Voreingestellt:

```
TrickleDataSize 1
```

Diese Option legt die Größe der Pakete fest, die WebGate bei Verwendung des Data-Tricklings an den Client sendet. Die Größe wird standardmäßig in Byte angegeben. Bei Bedarf kann dies durch Angabe eines optionalen Quantifizierers geändert werden: K (Kilobyte), M (Megabyte) oder G (Gigabyte).

1K entspricht beispielsweise 1024 Byte.

Reserve DataSize

ReserveDataSize

Example:

```
ReserveDataSize 1
```

Voreingestellt:

```
ReserveDataSize 1024
```

Mit dieser Option wird die Datenmenge festgelegt, die WebGate empfangen muss, bevor Daten per Data-Trickling an den Client weitergeleitet werden. Die Größe wird standardmäßig in Byte angegeben. Bei Bedarf kann dies durch Angabe eines optionalen Quantifizierers geändert werden: K (Kilobyte), M (Megabyte) oder G (Gigabyte). 1K entspricht beispielsweise 1024 Byte.

Beachten Sie, dass der Wert von `TrickleDataSize` kleiner sein muss als der von `ReserveDataSize`.

4.7.7 Prüf- und Filtereinstellungen

BlockOnError

BlockOnError

Syntax:

```
BlockOnError "YES|NO"
```

Voreingestellt:

```
BlockOnError YES
```

Dateien, bei deren Prüfung Verarbeitungsfehler auftreten, werden gesperrt.

Block Unsupported Archive

BlockUnsupportedArchive

Syntax:

```
BlockUnsupportedArchive "YES|NO"
```

Voreingestellt:

```
BlockUnsupportedArchive YES
```

Archive, die der Scanner nicht verarbeiten kann, werden gesperrt.

WSInitServer

WSInitServer

Example:

```
WSInitServer debian.home.com:80
```

Voreingestellt:

```
WSInitServer cobion.avira.com:80
```

Hiermit wird der Server festgelegt, der für die Initialisierung der Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung verwendet wird. Diese Option wird nur wirksam, wenn eine gültige Lizenz für WebGate Suite installiert ist. Normalerweise kann die Standardeinstellung übernommen werden.

LocalFilter

LocalFilter

Syntax:

```
LocalFilter "YES|NO"
```

Voreingestellt:

```
LocalFilter YES
```

Diese Option steuert die Verwendung des lokalen URL-Filters, der von der Avira-URL-Filterbibliothek implementiert wird. Der Filter ist bei allen WebGate- und WebGate Suite-Lizenzen standardmäßig aktiviert. Sie können ihn deaktivieren, indem Sie diese Option auf `NO` einstellen.

OnlineFilter

OnlineFilter

Syntax:

```
OnlineFilter "YES|NO"
```

Voreingestellt:

```
OnlineFilter YES
```

Dieses Option steuert die Verwendung der Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung. Die Bibliothek ist bei allen WebGate- und WebGate Suite-Lizenzen standardmäßig aktiviert. Sie können die Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung deaktivieren, indem Sie diese Option auf `NO` einstellen.

4.7.8 SNMP-Einstellungen

SNMP Recipient

SNMPRecipient

Beispiel:

```
SNMPRecipient snmp.example.com
```

Voreingestellt:

```
NONE
```

Diese Option legt den Host fest, der die von WebGate gesendeten SNMP-Traps empfängt. Ist diese Option deaktiviert, werden keine SNMP-Traps gesendet.

SNMPSender

SNMPSender

Beispiel:

```
SNMPSender 192.0.0.1
```

Voreingestellt:

```
SNMPSender 127.0.0.1
```

Mit dieser Option wird der Absender für SNMP-Traps festgelegt. Die IP-Adresse, die Sie hier angeben, wird in den SNMP-Traps als Absenderadresse verwendet. Wenn Sie einen Hostnamen angeben, wird die IP-Adresse mittels DNS-Lookup bestimmt.

SNMP Community

SNMPCommunity

Beispiel:

```
SNMPCommunity CompanyName
```

Voreingestellt:

```
SNMPCommunity Avira
```

Diese Option legt die Community-Zeichenfolge fest, die beim Senden von SNMP-Traps verwendet wird. Von WebGate gesendete Traps können nur SNMP-Hosts empfangen, die über diese Community-Zeichenfolge verfügen oder für die keine Community-Zeichenfolge festgelegt ist.

4.8 Client-Konfiguration

Nachdem WebGate gestartet wurde, muss das Programm in den Webbrowsern als HTTP/FTP-Proxy festgelegt werden (Netzwerkkonfiguration 0 und 1).

Wenn in Ihrem Netzwerk bereits ein HTTP/FTP-Proxy vorhanden ist und sich WebGate hinter dem Proxy befindet (Netzwerkkonfiguration 2), müssen nicht die Webbrowser-Einstellungen, sondern die Einstellungen des Proxys geändert werden (siehe 4.12 Proxy-Konfiguration).

4.9 URL-Filterung

Erlaubt Clients, ausgehende Anforderungen zu filtern. Die Filterung ist zweistufig angelegt.

Zunächst wird die URL-Filterbibliothek von Avira verwendet. Dabei wird anhand einer Liste bekannter URLs festgestellt, ob eine URL gefährlich ist. Für jede gefährliche URL wird eine der folgenden Kategorien zurückgegeben: Malware, Phishing oder Betrug. Ist die zurückgegebene Kategorie in der Option `BlockCategories` der Konfigurationsdatei angegeben, wird die Anforderung abgelehnt. Die Avira-URL-Filterbibliothek steht zur Verfügung, wenn eine gültige Lizenz für WebGate oder WebGate Suite vorhanden ist.

Wenn die URL nicht in der Avira-URL-Filterbibliothek enthalten ist oder nicht

durch die Konfigurationsdatei blockiert wird, wird die Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung verwendet. Diese Bibliothek filtert Anforderungen auf der Grundlage von URL-Kategorien.

Diese Funktion steht nur in der Avira AntiVir WebGate Suite zur Verfügung. Für die Bibliothek ist eine Schlüsseldatei erforderlich, die zur Verschlüsselung des Datenverkehrs benutzt wird. Jedes Kit enthält eine Schlüsseldatei. Sie befindet sich im Verzeichnis /usr/lib/AntiVir/webgate/wskeyfile.

Die URL-Filterung erfolgt erst, nachdem die Zugriffssteuerungsregeln (ACL) ausgewertet wurden. Eine URL, die durch diese Regeln getunnelt wird, wird unabhängig von ihrer Kategorie nicht gesperrt.

Die Avira-URL-Filterbibliothek und die Avira-Bibliothek für die Webzugriffs- und Inhaltssteuerung sperren eine Seite nur auf der Grundlage der URL. Anforderungen, die an eine IP-Adresse gerichtet sind (z. B. http://209.85.135.103/), werden von den Bibliotheken nicht gesperrt.

Die Kategorien, die von WebGate gesperrt werden, werden in der Konfigurationsdatei mit der Option `BlockCategories` in Form einer Nummernliste festgelegt.

In der folgenden Tabelle sind alle verfügbaren Kategorien zusammen mit ihren Nummern aufgeführt.

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

Nummer	Kategorie
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

Nummer	Kategorie
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

4.10 SNMP-Traps

WebGate kann so konfiguriert werden, dass der Administrator per SNMP-Traps über interne Fehler und Malware-Warnungen informiert wird. Die Definition dieser Traps steht in den MIB-Dateien zur Verfügung.

SNMP macht keine Vorgaben hinsichtlich der Informationen (Variablen), die ein verwaltetes System anbieten muss, sondern ermöglicht es, die verfügbaren Informationen in so genannten MIBs (Management Information Base) zu definieren. MIBs beschreiben die Struktur der Verwaltungsdaten eines Gerätesubsystems. Dabei wird ein hierarchischer Namensraum verwendet, der Objektbezeichner (OID) enthält.

WebGate stellt zwei MIB-Dateien mit einer Beschreibung der SNMP-Traps bereit, die das Programm senden kann:

```
AVIRA-MIB.txt
AVIRA-WEBGATE-V0-MIB.txt
```

Die MIB-Dateien werden bei der Installation in den Ordner /usr/lib/AntiVir/webgate/data kopiert. Sie können die Dateien entweder in den mibs-Ordner des SNMP-Agenten kopieren oder den SNMP-Agenten so konfigurieren, dass er im obigen Ordner nach MIB-Dateien sucht. Entsprechende Anleitungen finden Sie in der Dokumentation des SNMP-Agenten.

wgtUp

wgtUp

WebGate wurde gestartet.

wgtDown

wgtDown

WebGate wurde angehalten.

wgtAlert

wgtAlert

Der Scanner hat Malware gefunden.

wgtSuspicious

wgtSuspicious

Der Scanner konnte die Prüfung nicht beenden und WebGate hat die Anforderung als verdächtig eingestuft. Parameter: Der Grund für den Verdacht und die URL der Anforderung.

wgtMalware Scanner Unreach

wgtMalwareScannerUnreach

WebGate konnte keine Verbindung zum Malware-Scanner herstellen.

wgtMatched CategoryBy OnlineFilter

wgtMatchedCategoryByOnlineFilter

WebGate hat die Anforderung unter Verwendung des Online-Filters mit einer konfigurierten Kategorie verglichen. Parameter: Kategoriename und URL der verglichenen Kategorie.

Diese Funktion steht nur zur Verfügung, wenn eine Lizenz für WebGate Suite vorhanden ist.

wgtMatchedCategoryByRTPSFilter

wgtMatchedCategoryByRTPSFilter

WebGate hat die Anforderung unter Verwendung des RTPS-Filters mit einer konfigurierten Kategorie verglichen. Parameter: Kategoriename und URL der verglichenen Kategorie.

Diese Funktion steht nur zur Verfügung, wenn eine Lizenz für WebGate RTPS vorhanden ist.

wgtMatchedCategoryByLocalFilter

wgtMatchedCategoryByLocalFilter

WebGate hat die Anforderung unter Verwendung des Offline-Filters mit einer konfigurierten Kategorie verglichen. Parameter: Kategoriename und URL der verglichenen Kategorie.

wgtLicenseExpiredOrInvalid

wgtLicenseExpiredOrInvalid

Die WebGate-Lizenz ist abgelaufen oder ungültig.

wgtLicenseWillExpireSoon

wgtLicenseWillExpireSoon

Die Lizenz läuft in weniger als 30 Tagen ab. Parameter: Anzahl der Tage, die die Lizenz noch gültig ist.

4.11 WebGate-Zugriffssteuerung

WebGate implementiert ein Squid-ähnliches Zugangssteuerungsschema. Das Schema ist in einer eigenen Datei gespeichert, die in der Konfigurationsdatei angegeben ist (/etc/avira/avwebgate.conf.) Jede Zeile in dieser Konfigurationsdatei kann maximal 4096 Zeichen enthalten. WebGate stellt für die Zugriffssteuerung eine Untermenge von Squid bereit. Es ist auch möglich, einen Squid-Proxyserver zusammen mit WebGate auszuführen.

Wie bei Squid verwendet auch das Zugriffssteuerungsschema von WebGate zwei Komponenten: ACL-Elemente und Zugriffslisten.

4.11.1 ACL-Elemente

ACL-Elemente

ACL-Elemente

Ein ACL-Element hat das folgende Format:

```
acl <Name> <Typ> <Regel>
```

Jedes ACL-Element hat einen eindeutigen Namen. Sind mehrere Elemente mit demselben Namen vorhanden, wird ein Fehler gemeldet.

Das Element `all` *trifft auf jede Anforderung und Antwort zu und ist durch WebGate implizit definiert. Es kann nicht neu definiert werden.*

WebGate verwendet folgende Typen von ACL-Elementen

browser

Syntax:

```
acl <Name> browser [-i] <regulärer Ausdruck>
```

Dieses Element ermöglicht die Filterung von Verbindungen auf der Grundlage des Benutzeragenten. Das Flag `[-i]` sorgt für die Auswertung von `regulärer Ausdruck` ohne Berücksichtigung der Groß-/Kleinschreibung. Reguläre Ausdrücke, die mit `-i` und einem Leerzeichen beginnen, müssen mit `\-i` auskommentiert werden.

src

Syntax:

```
acl <Name> src <IP/Netzmaske>
acl <Name> src <IP1-IP2/Netzmaske>
```

Dieses Element ermöglicht die Filterung von Verbindungen auf der Grundlage der IP-Adresse. Sie können eine einzelne IP-Adresse oder einen Bereich mit IP-Adressen angeben. Zum Filtern mehrerer Adressen wird das logische `ODER` verwendet.

Beispiel:

```
acl <Name> src <IP1/Netzmaske IP2/Netzmaske IP3/
Netzmaske>
```

Das ACL-Element trifft zu, wenn mindestens eine IP-Adresse übereinstimmt.

port

Syntax:

```
acl <Name> port <Nummer>
acl <Name> port <Bereich>
```

Dieses Element ermöglicht die Filterung von Verbindungen auf der Grundlage des Zielports. Sie können einen einzelnen Port oder einen Portbereich angeben. Zum Filtern mehrerer Ports wird das logische `ODER` verwendet.

dstdomain

Syntax:

```
acl <Name> dstdomain <Domäne>
acl <Name> dstdomain "<Datei>"
```

Dieses Element ermöglicht die Filterung von Verbindungen auf der Grundlage der Zieldomäne. Zum Filtern mehrerer Domänen wird das logische `ODER` verwendet.

Beispiel:

```
acl antivir dstdomain .antivir.de
```

Das ACL-Element trifft zu für `*.antivir.de`
Sie können Domänen in einer Datei definieren, indem Sie sie durch Leerzeichen trennen oder in einer eigenen Zeile eingeben. Der Dateipfad muss in Anführungszeichen eingeschlossen werden.

dstdomain_regexp

Syntax:

```
acl <Name> dstdomain_regexp [-i] <regulärer Ausdruck>
acl <Name> dstdomain_regexp -f "/Pfad"
```

Dieses Element ermöglicht die Filterung von Verbindungen auf der Grundlage der Zieldomäne, wobei der Vergleich mithilfe regulärer Ausdrücke erfolgt.
Mit der Option `-f` können Sie eine Datei mit regulären Ausdrücken angeben. Der Pfad der Datei muss in Anführungszeichen eingeschlossen werden. Jede Zeile in der Datei steht für einen regulären Ausdruck. Sie muss das folgende Format haben: `[-i] <regulärer Ausdruck>`.

dsturi

Syntax:

```
acl URIS dsturi -f "path_to_list"
acl URI <uri>
```

Beispiel:

```
acl URIS dsturi -f "/etc/avira/list_of_uris.txt"
acl URI dsturi http://web.adresse.de
```

Dieses Element ermöglicht die Filterung von Verbindungen auf Grundlage der vollständigen Ziel-URIs/URLS. Zum Filtern mehrerer URIs/URLs wird das logische `ODER` verwendet. Der Pfad der Datei muss in Anführungszeichen eingeschlossen werden. Jede Zeile in der Datei stellt eine URI dar.

dsturi_regexp

Syntax:

```
acl URIS dsturi_regexp [-i] <regular expression>
acl URIS dsturi_regexp [-i] -f "path_to_list"
```

Beispiel:

```
acl URIS dsturi_regexp -i -f "list_of_regex.txt"
```

Dieses Element ermöglicht die Filterung von Verbindungen auf Grundlage der vollständigen Ziel-URI/URL, wobei der Vergleich mithilfe regulärer Ausdrücke erfolgt.
Mit der Option `-f` können Sie eine Datei mit regulären Ausdrücken angeben. Der Pfad der Datei muss in Anführungszeichen eingeschlossen werden. Jede Zeile in der Datei steht für einen regulären Ausdruck. Sie muss das folgende Format haben: `[-i] <regulärer Ausdruck>.`

req_mime_type

Syntax:

```
acl <Name> req_mime_type <regulärer Ausdruck>
```

Mit diesem Element kann der MIME-Header der Anforderung nach <regexp> durchsucht werden. Mithilfe dieses Elements können Datei-Uploads und HTTP-Tunnelanforderungen erkannt werden.

rep_mime_type

Syntax:

```
acl Name rep_mime_type reg exp
```

Mit diesem Element kann der MIME-Header der Antwort nach <regexp> durchsucht werden. Es kann zum Erkennen von Datei-Downloads verwendet werden. Wenn http_access-Regeln verwendet werden, ist dieses Element ungültig.

set

Syntax:

```
acl <Name> set <Option> <Wert>
```

Mit diesem Element kann eine Option für eine Anforderung oder eine Antwort definiert werden. In einer `http_access`- oder `http_reply_access`-Liste wird dieses Element immer zu `true` ausgewertet. Wenn die Anforderung mit der entsprechenden Zugriffsliste übereinstimmt, setzt das Element die gewünschte Option. Folgende Optionen können gesetzt werden:

```
TrickleDataSize, ReserveDataSize, KeepAliveMode,
RefreshInterval, RedirectInterval und KeepAliveInterval
```

Wenn die `http_access`*- oder* `http_reply_access`*-Regeldefinition sowohl* `ReserveDataSize` *als auch* `TrickleDataSize` *enthält, muss* `ReserveDataSize` *vor* `TrickleDataSize` *angegeben werden.*

Eine Timeout-Verhinderung, die mithilfe von ACL-Elementen definiert wird, setzt alle anderen diesbezüglichen Einstellungen in der Konfigurationsdatei außer Kraft.

4.11.2 Zugriffslisten

Zugriffslisten

Zugriffslisten

WebGate unterstützt zwei Squid-Zugriffslisten: `http_access` und `http_reply_access`. Eine Regel für eine Zugriffsliste besteht aus dem Regeltyp, der gewünschten Aktion und einer Liste mit ACL-Elementen.

http_access

Syntax:

```
http_access <allow|scan|deny|tunnel> <ACL_Name> ...
```

Diese Liste filtert Anforderungen auf der Grundlage von ACL-Übereinstimmungen. Zur Angabe mehrerer ACL-Namen wird das logische `UND` verwendet. Wenn keine Regel zutrifft (Regel „allow“), wird die Verbindung standardmäßig zugelassen, aber die Daten werden geprüft. Wenn alle Anforderungen außer den oben angegebenen abgelehnt werden sollen, muss die Regel „http_access deny all“ hinzugefügt werden.

http_reply_access

Syntax:

```
http_reply_access <allow|scan|deny|tunnel> <ACL_Name>
...
```

Diese Liste filtert Serverantworten auf der Grundlage von ACL-Übereinstimmungen. Folgende Aktionen können definiert werden:

allow

Die Anforderung wird zugelassen und an die nachgelagerten Module (URL-Filterung und Prüfung) übergeben.

scan

Die Anforderung wird zugelassen und direkt an das Prüfmodul übergeben. URL-Filter bleiben unberücksichtigt.

deny

Die Anforderung wird von WebGate blockiert.

tunnel

Die Daten werden weitergeleitet und WebGate greift nicht in die Transaktion ein.

Da keine Prüfung der Daten erfolgt, sollte die Aktion „tunnel“ mit Bedacht verwendet werden.

4.12 Proxy-Konfiguration

Wenn WebGate „hinter“ einem Proxyserver (Netzwerkkonfiguration 2) oder zwischen zwei Proxys installiert ist, muss der Proxy so konfiguriert werden, dass er alle Anforderungen an WebGate weiterleitet (WebGate fungiert also als übergeordneter Proxy).

4.12.1 Squid als Proxy

Das folgende Beispiel zeigt die Konfiguration des Squid-Proxyservers.

Damit Squid ALLE Anforderungen an Avira AntiVir WebGate weitergibt, sind folgende Einträge in der Konfigurationsdatei squid.conf erforderlich:

```
cache_peer <WebGateHost> parent <WebGatePort> 0 no-query no-
digest default
acl all src all
never_direct allow ALL
```

<WebGateHost> und <WebGatePort> sind durch die entsprechenden Werte zu ersetzen.

Über SSL-Tunnelverbindungen (mit der HTTP-CONNECT-Methode eingerichtet) übertragene Daten werden von WebGate NICHT geprüft. Wenn der Proxy auch für HTTPS verwendet wird, können Sie veranlassen, dass er WebGate bei diesen Verbindungen umgeht. Dies geschieht mit der folgenden Konfiguration (squid.conf):

```
cache_peer <WebGateHost> parent <WebGatePort> 0 no-query no-
digest default
acl SSL method CONNECT
acl all src all
always_direct allow SSL
never_direct allow ALL
```

Alternativ können Sie Squid auch explizit anweisen, nur HTTP- und FTP-Anforderungen an WebGate zu übergeben und WebGate bei allen anderen Anforderungstypen zu umgehen (squid.conf):

```
cache_peer <WebGateHost> parent <WebGatePort> 0 no-query no-
digest default
acl SCAN_ACL proto HTTP
acl SCAN_ACL proto FTP
cache_peer_access <WebGateHost> allow SCAN_ACL
cache_peer_access <WebGateHost> deny !SCAN_ACL
never_direct allow SCAN_ACL
```

Wenn WebGate als übergeordneter Proxy verwendet wird, muss WebGate vor dem Proxy gestartet werden.

4.12.2 Squid-ICAP verwenden

WebGate kann auch im ICAP-Modus verwendet werden (mit Squid-ICAP). Da ICAP jedoch keinen Mechanismus für die Timeout-Verhinderung bereitstellt, ist diese Verwendung von WebGate in vielen Situationen nicht geeignet.
Der integrierte ICAP-Support steht ab Squid 3.0 oder höher zur Verfügung. Es besteht auch die Möglichkeit für Squid 2.6 und 2.7 einen Patch einzuspielen.
Damit WebGate mit Squid-ICAP arbeiten kann, sind folgende Einträge in der Datei squid(3).conf erforderlich:

```
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
```

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

4.12.3 Apache als Proxy

Wenn Sie WebGate zusammen mit einem Apache-Proxy (`mod_proxy`) verwenden möchten, können Sie WebGate wie folgt als Remote-Proxy konfigurieren (httpd.conf):

```
ProxyRequests On
ProxyRemote http http://<WebGateHost>:<WebGatePort>
ProxyRemote ftp http://<WebGateHost>:<WebGatePort>
```

<WebGateHost> und <WebGatePort> sind durch die entsprechenden Werte zu ersetzen.

5 Betrieb

Nach Abschluss der Installation und Konfiguration und nach dem Start von Avira AntiVir WebGate ist die lückenlose Überwachung Ihres Systems durch WebGate gewährleistet. Der laufende Betrieb kann gelegentliche Änderungen an der Konfiguration erfordern. Erläuterungen dazu finden Sie im Kapitel Konfiguration.

Dieses Kapitel besteht aus folgenden Abschnitten:

„Avira AntiVir WebGate manuell starten und beenden“ beschreibt, wie WebGate von der Konsole aus gestartet und beendet wird.

In „Vorgehen beim Erkennen von Viren oder unerwünschten Programmen“ erfahren Sie, wie Sie sich verhalten müssen, wenn Ihr Netzwerk infiziert ist.

5.1 Avira AntiVir WebGate manuell starten und beenden

Hinweis: *Um Avira AntiVir WebGate manuell zu starten oder zu beenden, müssen Sie als* ***root****-Benutzer angemeldet oder mit den erforderlichen Berechtigungen ausgestattet sein.*

Wenn Sie WebGate nach der Beschreibung in Avira AntiVir WebGate installieren – Seite 12 installiert haben, wird es beim Systemstart automatisch gestartet.

Avira AntiVir WebGate starten

Geben Sie Folgendes ein:

```
/usr/lib/AntiVir/webgate/avwebgate start
```

Das Programm wird mit der folgenden Meldung gestartet:

```
Starting AVIRA AntiVir WebGate ...
Starting: savapi
Starting: avwebgate.bin
```

Wenn Sie bei der Installation festgelegt haben, dass WebGate automatisch gestartet werden soll, brauchen Sie sich darum nicht zu kümmern.

Dies ist der empfohlene Weg, um WebGate zu starten.

Wenn Sie für die Binärdatei avwebgate.bin andere Parameter verwenden möchten, ändern Sie im Skript avwebgate die Variable DAEMONPARAMS.

Kommandozeilenparameter

avwebgate.bin -C <file>	Spezifiziert eine zusätzliche Konfigurationsdatei (Voreingestellt ist: /etc/avira/avwebgate.conf)
-N	Startet WebGate ohne daemonizing
-D	Setzt die Debug-Ausgab(DebugLevel 0-7)

-V, --version	Zeigt die WebGate Versionsnummer an
--filter-version	Zeigt Informationen über den verwendeten Scanner und die Filter
--status	Zeigt, ob WebGate entsprechend der Konfiguration läuft
--dump-config	Zeigt die aktuellen aktivierten Konfigurationswerte
--help	Zeigt die Liste der Optionen mit ihren Beschreibungen

Ohne gültigen Lizenzschlüssel kann WebGate nicht gestartet werden.

Um einen Testschlüssel anzufordern, senden Sie eine Email an sales@avira.com

Hinweis: *Beim Herunterladen großer Dateien stellen Browser keinen Fortschritt fest, wenn die* `Refresh`*-Methode zum Verhindern von Timeouts deaktiviert ist (Standardeinstellung). Der Grund dafür ist, dass WebGate die gesamte Datei herunterlädt und prüft, bevor die ersten Daten zum Client gesendet werden.*

Nach der Prüfung wird die gesamte Datei sehr schnell zum Client gesendet (über das LAN).

Avira AntiVir WebGate beenden

Geben Sie Folgendes ein:

```
/usr/lib/AntiVir/webgate/avwebgate stop
```

Das Programm wird mit der folgenden Meldung beendet:

```
Stopping AVIRA AntiVir WebGate ...
Stopping: avwebgate.bin
Stopping: savapi
```

AntiVir WebGate neu starten

Ein Neustart ist erforderlich, wenn Sie beispielsweise Änderungen an Konfigurationsskripts vorgenommen haben.

Geben Sie Folgendes ein:

```
/usr/lib/AntiVir/webgate/avwebgate restart
```

Das Programm zeigt zuerst die folgende Meldung an und startet dann neu:

```
Stopping AVIRA AntiVir WebGate ...
Stopping: avwebgate.bin
Stopping: savapi
Starting AVIRA AntiVir WebGate ...
Starting: savapi
Starting: avwebgate.bin
```

AntiVir WebGate-Status prüfen

Geben Sie Folgendes ein:

```
/usr/lib/AntiVir/webgate/avwebgate status
```

Das Programm zeigt Informationen über die WebGate-Daemons an:

```
Status: avwebgate.bin running
Status: savapi running
```

5.2 Avira AntiVir WebGate testen

Nach dem Abschluss der Installation und Konfiguration können Sie die Funktionalität von AntiVir WebGate mit einem Testvirus überprüfen. Der Virus richtet keinerlei Schaden an, löst aber bei der Prüfung des Computers eine Reaktion des Sicherheitsprogramms aus.

Avira AntiVir WebGate mit einem Testvirus überprüfen

Starten Sie WebGate:

```
/usr/lib/AntiVir/webgate/avwebgate start
```

Geben Sie in Ihrem Webbrowser die URL http://www.eicar.org ein.

Lesen Sie die Informationen über den Testvirus eicar.com.

Laden Sie den Testvirus auf Ihren Computer herunter.

Avira AntiVir WebGate blockiert den Zugriff auf die Datei und gibt im Browser eine Warnung aus:

In der Logdatei finden Sie detaillierte Informationen über den Vorfall.

5.3 Vorgehen beim Erkennen von Viren oder unerwünschten Programmen

Wenn Avira AntiVir WebGate richtig konfiguriert ist, werden alle Aufgaben auf Ihrem Computer automatisch erledigt:

Die infizierte Datei wird repariert oder zumindest gelöscht.

Wenn die Datei nicht repariert werden konnte, wird der Zugriff darauf blockiert und die Datei je nach Konfiguration umbenannt oder verschoben. Dadurch wird die Gefahr einer Infektion beseitigt.

In jedem Fall sollten Sie die folgenden Maßnahmen ergreifen:

Versuchen Sie herauszufinden, durch welche „Hintertür“ Ihr System infiziert wurde.

Prüfen Sie gezielt die Datenträger, die infiziert sein könnten.

Informieren Sie Ihr Team, Ihre Vorgesetzten und Ihre Geschäftspartner.

Informieren Sie Ihren Systemadministrator und Ihren Sicherheitsanbieter.

Infizierte Dateien an Avira Operations GmbH & Co. KG senden

Senden Sie uns die Malware oder die verdächtigen Dateien zu, die von unseren Produkten noch nicht erkannt oder entfernt werden. Komprimieren Sie den Virus oder die verdächtige Datei in einem Archiv (gzip, WinZIP, PKZip, Arj), und senden Sie dieses Archiv als Email-Anhang an virus@antivir.de.

Achtung: *Verwenden Sie beim Komprimieren das Passwort* `virus`. *So wird die Datei nicht von Virenscannern auf Email-Gateways gelöscht.*

6 Aktualisierungen

Mit Avira Updater können Sie die Avira-Software auf Ihrem Computer über die Avira-Update-Server aktualisieren. Das Programm kann entweder durch Bearbeiten der Konfigurationsdatei (Updater-Konfiguration in avupdate-webgate.conf) oder über Parameter in der Befehlszeile konfiguriert werden.

Es wird empfohlen, Updater als **root** auszuführen. Wenn Updater nicht als **root** ausgeführt wird, fehlen dem Programm die notwendigen Berechtigungen zum Neustart der Avira AntiVir WebGate-Daemons, und der Neustart muss manuell als **root** durchgeführt werden.

Dies hat den Vorteil, dass alle laufenden Prozesse von Avira AntiVir WebGate-Daemons (z. B. Scanner, Engine, WebGate) automatisch mit den neuesten Antivirendateien aktualisiert werden, ohne die laufenden Prüfprozesse zu unterbrechen. Dadurch ist sichergestellt, dass alle Dateien geprüft werden.

6.1 Internet-Aktualisierungen

Manuell

Wenn Sie Avira AntiVir WebGate oder einige seiner Komponenten aktualisieren möchten:
Verwenden Sie den folgenden Befehl:

```
/usr/lib/AntiVir/webgate/avupdate-webgate
--product=webgate
```

Als `[Produkt]` können Sie Folgendes eingeben:

- `Scanner` – Der Scanner, die Engine und die VDF-Dateien werden aktualisiert (empfohlen).
- `WebGate` – Vollständige Aktualisierung (WebGate, Scanner, Engine und VDF-Dateien).

Wenn Sie nur nach einer neuen AntiVir-Version suchen möchten, ohne AntiVir WebGate zu aktualisieren:
Verwenden Sie den folgenden Befehl:

```
/usr/lib/AntiVir/webgate/avupdate-webgate --check
--product=webgate
```

Automatische Aktualisierungen mit dem cron-Daemon

Regelmäßige Aktualisierungen werden mit dem cron-Daemon durchgeführt.

Die Einstellungen für automatische Aktualisierungen in /etc/crontab **sind bereits eingetragen, wenn** Avira AntiVir WebGate mit dem install-Skript installiert und die Rückfrage, ob AntiVir Updater installiert und automatisch gestartet werden soll, mit `Ja` beantwortet wurde.

Weitere Informationen über den cron-Daemon finden Sie in Ihrer UNIX-Dokumentation.

So können Sie die Einstellungen für automatische Aktualisierungen in der crontab-Datei manuell festlegen oder ändern:

Fügen Sie der Datei /etc/cron.d/avira_updater den gewünschten Eintrag hinzu oder bearbeiten Sie ihn (siehe folgendes Beispiel).

Beispiel: Um die Aktualisierung stündlich (immer um *:23) durchzuführen, geben Sie den folgenden Befehl ein:

```
23 * * * * root /usr/lib/AntiVir/webgate/avupdate-webgate
--product=[Produkt]
```

Als `[Produkt]` können Sie Folgendes eingeben:

- `Scanner` – Der Scanner, die Engine und die VDF-Dateien werden aktualisiert (empfohlen).
- `WebGate` – Vollständige Aktualisierung (WebGate, Scanner, Engine und VDF-Dateien).

Starten Sie den Aktualisierungsprozess, um die Einstellungen zu überprüfen:

```
/usr/lib/AntiVir/webgate/avupdate-webgate
--product=[Produkt]
```

Die Werte für `[Produkt]` sind die gleichen wie im obigen Beispiel.

War die Aktualisierung erfolgreich, wird ein Bericht in die Logdatei /var/log/avupdate-webgate.log geschrieben.

7 Service

7.1 FAQs

7.1.1 Überwachung von SNMP Traps unter Debian 5

1.) Installieren Sie das snmpd Paket:

```
$ apt-get install snmpd
```

2.) Kopieren Sie die MIB-Dateien des Avira AntiVir WebGate Pakets in einen Ordner:

```
$ cp antivir-webgate-prof-<Version>/etc/AVIRA-*-
MIB.txt  /usr/share/snmp/mibs
```

3.) Konfigurieren Sie snmpd so, dass die WebGate MIB-Dateien gelesen werden:

```
$ echo "+mibs AVIRA-MIB" >> /etc/snmp/snmp.conf
$ echo "+mibs AVIRA-WEBGATE-V0-MIB" >>
/etc/snmp/snmp.conf
```

4.) Konfigurieren Sie snmpd, indem Sie /etc/snmp/snmptrapd.conf editieren. Geben Sie an, dass WebGates SNMP Traps akzeptiert werden sollen:

```
$ echo "authCommunity log,execute,net SNMP_COMMUNITY" >>
/etc/snmp/snmptrapd.conf
```

Ersetzen Sie SNMP_COMMUNITY mit dem für die SNMPCommunity Option gültigen Wert (voreingestellt `Avira`).

Anschließend konfigurieren Sie snmptrapd so, dass bei Empfang einer bestimmten SNMP Trap ein benutzerdefiniertes Programm aufgerufen wird.

Mit folgender Zeile beispielsweise

```
traphandle AVIRA-WEBGATE-V0-MIB::wgtAlert /usr/local/
bin/webgate_alert
```

wird snmptrapd jedes Mal /usr/local/bin/webgate_alert ausführen, wenn eine `wgtAlert` Trap empfangen wird.

/usr/local/bin/webgate_alert kann z.B. folgendermaßen aussehen:

```
#!/bin/bash

name=
url=

while read oid val
do
  if [ "$oid" = "AVIRA-WEBGATE-V0-MIB::wgtMalwareName.0" ]
  then
    name=$val
  fi

  if [ "$oid" = "AVIRA-WEBGATE-V0-MIB::wgtRequestURL.0" ]
  then
    url=$val
  fi
 done

echo "WebGate found $name when accessing $url"
```

5.) Führen Sie
`$ snmptrapd -f-c /etc/snmp/snmptrapd.conf -M /usr/share/snmp/mibs -m AVIRA-MIB:AVIRA-WEBGATE-V0-MIB`
aus, und warten Sie bis AntiVir WebGate die `wgtAlert` Trap versendet (Sie könnten z.B. den Eicar Test Virus durch AntiVir WebGate verschicken, um ein Versenden der Trap auszulösen).

Im Terminal, in dem Sie snmptrapd gestartet haben, sollte nun Folgendes zu lesen sein:

```
WebGate found "Eicar-Test-Signature ; virus ; Contains
code of the Eicar-Test-Signature virus" when accessing
"http://www.eicar.org/download/eicar.com"
```

7.2 Support

Auf unserer Website http://www.avira.com finden Sie alle erforderlichen Informationen zu unserem umfangreichen Support-Service.

Nutzen Sie die Kompetenz und Erfahrung unserer Entwickler. Die Experten der Avira GmbH beantworten Ihre Fragen und können Ihnen bei kniffligen technischen Problemen weiterhelfen.

In den ersten 14 Tagen nach Erwerb einer Lizenz haben Sie die Möglichkeit, den **AntiVir Installationssupport** in Anspruch zu nehmen – telefonisch, per Email oder über das Online-Formular.

Weitere Informationen über den Support für unser Produkt finden Sie unter http://www.avira.com/de/support-for-business.

Bevor Sie sich über unsere Hotline mit uns in Verbindung setzen, empfehlen wir Ihnen, zunächst den Bereich „Häufig gestellte Fragen“ unter http://www.avira.com/de/support-for-business-faq zu besuchen.

Nehmen Sie kostenlos an unserem Message Board teil, das Sie unter http://forum.antivir.de finden.
Nutzen Sie die Suchoption, denn möglicherweise sind Ihre Fragen schon von anderen Benutzern gestellt und im Message Board beantwortet worden.

Support per Email erhalten Sie unter der Adresse http://www.avira.com.

7.3 Online-Shop

Sie möchten unsere Produkte bequem per Mausklick einkaufen?

Im Online-Shop der Avira GmbH können Sie unter http://www.avira.com schnell und sicher Lizenzen erwerben, erweitern oder verlängern. Sie werden schrittweise durch das Bestellmenü geführt. Ein **mehrsprachiges Customer-Care-Center** informiert Sie über den Bestellprozess, die Zahlungsabwicklung und die Auslieferung. Wiederverkäufer können auf Rechnung bestellen und ein Reseller-Panel nutzen.

7.4 Kontakt

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

Weitere Informationen über uns und unsere Produkte finden Sie unter http://www.avira.com.

8 Anhang

8.1 Glossar

Begriff	Bedeutung
Backdoor (BDC)	Ein Backdoor-Programm ist ein infiltrantes Programm, das ohne Wissen des Benutzers Daten vom Computer stiehlt. Dieses Programm wird von Dritten manipuliert, die aus der Ferne Backdoor-Steuersoftware über das Internet oder das Netzwerk nutzen. AntiVir erkennt Backdoor-Steuerprogramme.
cron (Daemon)	Ein Daemon, der zu vorgegebenen Zeiten andere Programme startet.
Daemon	Ein im Hintergrund laufender Prozess zur Systemverwaltung unter Unix. Im Durchschnitt werden auf einem Rechner einige Dutzend Daemons ausgeführt. Diese Prozesse werden normalerweise zusammen mit dem Rechner gestartet und heruntergefahren.
Dialer	Ein Einwahlprogramm mit Zahlungsverpflichtung. Wenn ein Dialer auf Ihrem Computer installiert wurde, richtet er eine teure Internet-Verbindung ein, die hohe Kosten verursacht. Dies kann zu extrem hohen Telefonrechnungen führen. AntiVir erkennt Dialer.
Engine	Das Prüfmodul der AntiVir-Software.
Heuristik	Ein systematischer Prozess zur Lösung eines Problems unter Nutzung allgemeiner und spezifischer Regeln, die auf Erfahrungswerten basieren. Eine Lösung ist jedoch nicht garantiert. AntiVir verwendet einen heuristischen Prozess zur Erkennung unbekannter Makroviren. Wenn typische virusartige Funktionen erkannt werden, wird das Makro als „verdächtig“ klassifiziert.
IUM	Avira Internet Update Manager. Die einzelnen Clientrechner in Ihrem Netzwerk müssen Updates nicht selber über das Internet durchführen, sondern werden bequem über Ihr Intranet aktualisiert.
Kernel	Die Basiskomponente eines Unix-Betriebssystems, die elementare Funktionen ausführt (z. B. Arbeitsspeicher- und Prozessverwaltung).
Logdatei	Auch: Berichtdatei. Eine Datei mit Berichten, die vom Programm zur Laufzeit generiert werden, wenn bestimmte Ereignisse eintreten.
Malware	Ein Oberbegriff für „Fremdkörper“ jeder Art. Dies können Störungen wie z. B. Viren sein, aber auch andere Software, die vom Benutzer im Allgemeinen als unerwünscht betrachtet wird (siehe auch „Unerwünschte Programme“).
Quarantäneverzeichnis	Das Verzeichnis, in dem infizierte Dateien gespeichert werden, damit der Benutzer nicht darauf zugreifen kann.

Begriff	Bedeutung
root	Ein Benutzer mit unbeschränkten Zugriffsrechten (z. B. der Systemadministrator unter Windows).
SAVAPI	Secure AntiVirus Application Programming Interface
Signatur	Eine Byte-Kombination, die zur Erkennung eines Virus oder eines unerwünschten Programms verwendet wird.
Skript	Eine Textdatei mit Befehlen, die vom System ausgeführt werden (ähnlich einer Batchdatei unter DOS).
SMC	Avira Security Management Center
SMP (Symmetrisches Multi Processing)	Unix SMP: Unix-Version für Computer mit Parallelprozessoren.
SMTP	Simple Mail Transfer Protocol: Ein Protokoll zur Übertragung von Emails im Internet.
syslog-Daemon	Ein Daemon, der von Programmen zur Protokollierung unterschiedlicher Informationen verwendet wird. Die Berichte werden in verschiedene Logdateien geschrieben. Der syslog-Daemon wird in der Datei /etc/syslog.conf konfiguriert.
Unerwünschte Programme	Ein Oberbegriff für Programme, die ohne Zustimmung des Benutzers oder Administrators installiert wurden und daher unerwünscht sind, obwohl sie auf dem Rechner keinen direkten Schaden anrichten. Dazu zählen u. a. Backdoor-Programme, Dialer, Witzprogramme und Spiele. AntiVir erkennt verschiedene Arten unerwünschter Programme.
VDF (Virus Definition File)	Eine Datei mit bekannten Signaturen von Viren und unerwünschten Programmen. In vielen Fällen ist es für eine Aktualisierung ausreichend, die neueste Version dieser Datei zu laden.

8.2 Weitere Informationen

Weitere Informationen zu Viren, Würmern, Makroviren und anderen unerwünschten Programmen finden Sie unter http://www.avira.com.

8.3 Goldene Regeln zum Schutz vor Viren

Erstellen Sie immer Startdisketten für Ihre Netzwerkserver und Workstations.

Nehmen Sie Disketten am Ende der Arbeit immer aus dem Laufwerk. Auch Disketten ohne ausführbare Programme können Programmcode im Bootsektor enthalten und dadurch Träger eines Bootsektorvirus sein.

Legen Sie regelmäßig Backups Ihrer Daten an.

Beschränken Sie den Austausch von Programmen. Dies gilt insbesondere für andere Netzwerke, Mailboxen, das Internet und Bekannte.

Prüfen Sie neue Programme vor der Installation, und führen Sie danach eine Prüfung des Datenträgers durch. Liegt das Programm komprimiert vor, lässt sich ein Virus in der Regel erst nach dem Entpacken und bei der Installation finden.

Haben andere Personen Zugang zu Ihrem Rechner, sollten Sie zum Schutz vor Viren folgende Regeln beachten:

Stellen Sie einen Testrechner bereit, auf dem Sie Software-Downloads, Demoversionen und virenverdächtige Datenträger (Disketten, CD-R, CD-RW, Wechsellaufwerke) untersuchen können.

Trennen Sie den Testrechner vom Netzwerk!

Benennen Sie einen Beauftragten, der bei einer Virusinfektion für die entsprechenden Aktivitäten verantwortlich ist, und bestimmen Sie alle zur Beseitigung eines Virus notwendigen Schritte.

Erstellen Sie einen Notfallplan. Ein solcher Plan kann Schäden/Verluste durch mutwillige Zerstörung, Diebstahl, Ausfall oder Veränderungen durch Inkompatibilität verhindern. Programme und Speichergeräte lassen sich ersetzen, nicht aber Daten, die für das wirtschaftliche Überleben eines Unternehmens notwendig sind.

Erstellen Sie einen Schutz- und Wiederherstellungsplan für Ihre Daten.

Sorgen Sie für ein einwandfrei konfiguriertes Netzwerk, und weisen Sie Zugriffsrechte nach vernünftigen Gesichtspunkten zu.

Diese Maßnahmen tragen zu einem wirksamen Schutz vor Viren bei.

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