

WatchGuard® Gateway AntiVirus™ Guide

Gateway AntiVirus™ for WatchGuard System Manager 7.5



Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2007 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the *WatchGuard System Manager User Guide*.

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

WFS Software Number v7.5
Document Version: 7.5

Contents

About Virus Signatures	2
Gateway AntiVirus Procedures	2
Installing Gateway AntiVirus	3
Enabling Gateway AntiVirus	4
Getting Gateway AntiVirus Status and Updates	5
<i>Seeing Gateway AntiVirus status</i>	5
<i>Updating Gateway AntiVirus signatures</i>	5
<i>Updating the antivirus engine</i>	6
<i>Clear Gateway AntiVirus statistics</i>	6
<i>Renew Gateway AntiVirus Licenses</i>	7
<i>AntiVirus License expiration</i>	7
Configuring Gateway AntiVirus System Settings	7
<i>Configure Gateway AntiVirus</i>	8
Configuring Gateway AntiVirus in the SMTP Proxy	9
<i>Add an SMTP Proxy with Gateway AntiVirus</i>	9
<i>Configure Gateway AntiVirus for an existing SMTP Proxy</i> ...	12
Using Gateway AntiVirus with More Than One Proxy	14
Gateway AntiVirus Headers	14
Monitoring Gateway AntiVirus Activity	15

WatchGuard Gateway AntiVirus™ Guide

Viruses are malicious computer programs that try to attack your computer or computers on your network. Viruses can be dangerous, and they can cause damage to files and resources. Some viruses find passwords and other sensitive information, and some can use your system or network to attack other systems.

WatchGuard® Gateway AntiVirus stops viruses before they get to computers on your network. Gateway AntiVirus uses the WatchGuard SMTP Proxy. When you enable Gateway AntiVirus, the WatchGuard SMTP Proxy looks at e-mail messages, finds viruses, and removes them.

NOTE

Gateway AntiVirus works with the SMTP Proxy. If your organization does not use SMTP to get e-mail, Gateway AntiVirus does not give virus protection.

Gateway AntiVirus finds viruses encoded with common e-mail attachment methods. These include base64, binary, 7-bit and 8-bit encoding. Gateway AntiVirus does not find viruses in uuencoded or binhex-encoded messages.

About Virus Signatures

When a new virus is identified on the Internet, the features that make the virus unique are identified and recorded. The features that make a virus unique are known as the virus signature. Gateway AntiVirus uses these virus signatures to find viruses. Gateway AntiVirus includes more than 40,000 virus signatures in the default configuration.

New viruses appear on the Internet frequently. To make sure that Gateway AntiVirus gives your network the best protection, you must update the virus signatures frequently. You can configure the Firebox® to update virus signatures automatically from WatchGuard. You can also update virus signatures manually on your Firebox. These updates are made available when new viruses are identified.

NOTE

You must keep virus signatures current to get the best protection from Gateway AntiVirus. However, new virus threats appear frequently. WatchGuard cannot guarantee that our product will stop every virus, or prevent damage to your systems or networks from a virus.

Gateway AntiVirus Procedures

To use Gateway AntiVirus, you must do these steps:

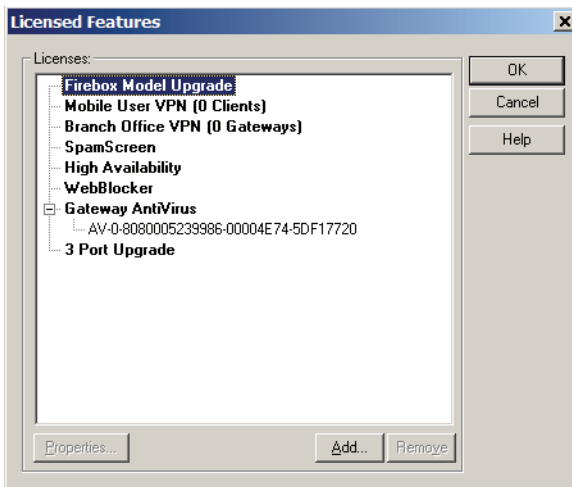
- 1 Install the Gateway AntiVirus feature. See “Installing Gateway AntiVirus” on page 3.
- 2 Enable the Gateway AntiVirus feature. See “Enabling Gateway AntiVirus” on page 4.
- 3 Update Gateway AntiVirus for the first time. See “Getting Gateway AntiVirus Status and Updates” on page 5.
- 4 Configure Gateway AntiVirus system settings. See “Configuring Gateway AntiVirus System Settings” on page 7.
- 5 Configure Gateway AntiVirus in the SMTP Proxy. See “Configuring Gateway AntiVirus in the SMTP Proxy” on page 9.

Installing Gateway AntiVirus

To install Gateway AntiVirus, you must have:

- A Gateway AntiVirus license key.
- An SMTP e-mail server behind the Firebox.
- The SMTP Proxy. For information on how to add the SMTP Proxy, see “Configuring Gateway AntiVirus in the SMTP Proxy,” on page 9.

- 1 From Policy Manager, select **Setup > Licensed Features**. The Licensed Features dialog box appears.

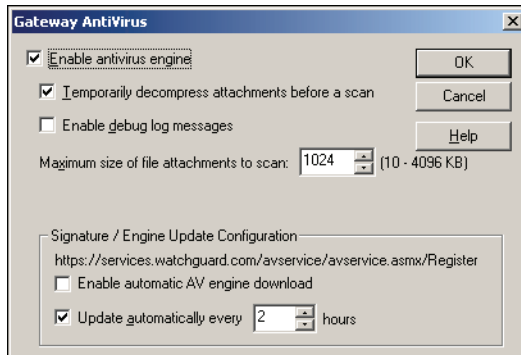


- 2 Click **Add**.
- 3 In the **Add/Import License Keys** dialog box, type or paste your license key. You can click **Browse** to find it on your computer or network. Click **OK**. The license key appears on the Licensed Features dialog box.

Enabling Gateway AntiVirus

Before you configure and use Gateway AntiVirus, you must enable Gateway AntiVirus on your Firebox. To do this:

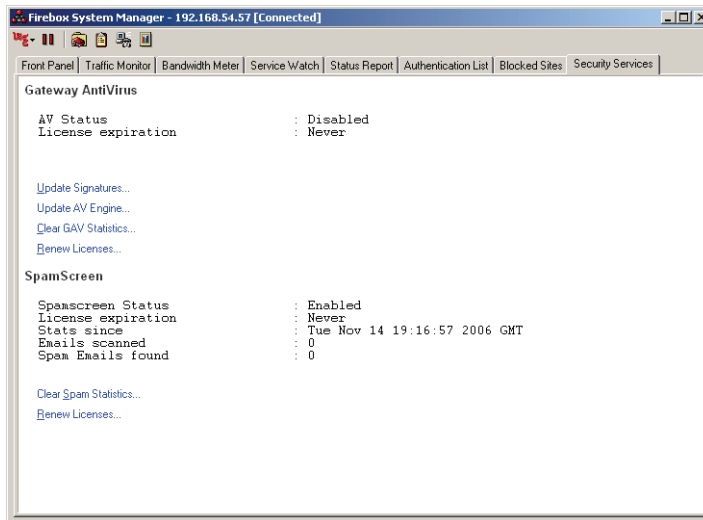
- 1 Click **Start > Programs > WatchGuard > Firebox System Manager**.
- 2 In the Connect to Firebox dialog box, type the IP address and status passphrase for the Firebox.
- 3 Click the Policy Manager button to start Policy Manager. You can select **Tools > Policy Manager** from the WatchGuard menu to start Policy Manager.
- 4 In Policy Manager, select **Setup > Gateway AntiVirus**. The Gateway AntiVirus window appears.



- 5 Select the **Enable antivirus engine** check box. Click **OK**.
- 6 Select **File > Save > To Firebox**.
The first time you enable the antivirus engine, you must save the configuration to the Firebox.
- 7 Type your configuration passphrase.
- 8 Click **OK**.

Getting Gateway AntiVirus Status and Updates

You can see the status and get updates for Gateway AntiVirus on the Security Services tab in the Firebox System Manager.



Seeing Gateway AntiVirus status

Gateway AntiVirus status tells you if Gateway AntiVirus protection is enabled. You can also see when the license expires and information about the virus scanner and the virus signatures.

To see Gateway AntiVirus status:

- 1 Start Firebox System Manager.
- 2 Click on the Security Services tab.
Gateway AntiVirus status appears. You only see Gateway AntiVirus status after you install the Gateway AntiVirus license.

Updating Gateway AntiVirus signatures

Gateway AntiVirus is automatically configured to update the antivirus signatures every two hours. See “Configure Gateway AntiVirus” on page 8 to change this setting. You can also update signatures manually. If the virus signatures are not current, you are not protected from the latest viruses.

To update Gateway AntiVirus manually:

- 1 Start Firebox System Manager.
- 2 Click on the Security Services tab.
Gateway AntiVirus status appears.
- 3 Click **Update Signatures**.
The Firebox downloads the latest available signature update for Gateway AntiVirus. You can see information about the update in Traffic Monitor.

You can configure Gateway AntiVirus to update virus signatures automatically. See “Configure Gateway AntiVirus” on page 8 for more information.

Updating the antivirus engine

WatchGuard may periodically make antivirus engine updates available for Gateway AntiVirus. When an engine update is made available, you will be notified by a LiveSecurity bulletin e-mail.

It is critical that you update your engine as soon as a new engine is available. Newer signatures may only work with newer antivirus engines. You have access to new engines for the term of your Gateway Antivirus subscription.

To update the Gateway AntiVirus engine manually:

- 1 Start Firebox System Manager.
- 2 Click on the Security Services tab.
Gateway AntiVirus status appears.
- 3 Click **Update AV Engine**.
The Firebox downloads the latest Gateway AntiVirus engine. You can see information about the update in Traffic Monitor.

You can configure Gateway AntiVirus to download engine updates automatically. See “Configure Gateway AntiVirus” on page 8 for more information.

Clear Gateway AntiVirus statistics

Clear Gateway AntiVirus statistics to see only new statistics.

To clear Gateway AntiVirus statistics:

- 1 Start Firebox System Manager.
- 2 Click on the Security Services tab.
Gateway AntiVirus status appears.
- 3 Click **Clear GAV Statistics**.

- 4 You are prompted for the configuration passphrase. Type the configuration passphrase and click **OK**.

The statistics are cleared and the Firebox starts to record statistics again. The **Stats since** field shows the last time and date that the statistics were cleared. The **Files scanned** and **Viruses found** fields show zeroes until a new file is examined or a virus is found.

NOTE

After you clear statistics, you can still see older log messages in the log files.

Renew Gateway AntiVirus Licenses

You can go to the web page to renew your Gateway AntiVirus license from Firebox System Manager.

To renew the license:

- 1 Start Firebox System Manager.
- 2 Click on the Security Services tab.
Gateway AntiVirus status appears.
- 3 Click **Renew Licenses**.
A web browser window starts with the license renewal page open. You must log in to your LiveSecurity account to view this page.

AntiVirus License expiration

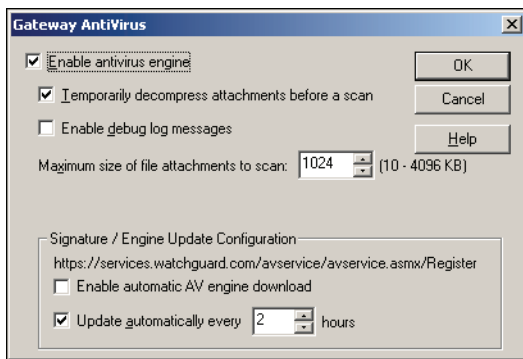
When a Gateway AntiVirus license expires, all Gateway Antivirus features stop working. You must add a new or upgrade license to resume AntiVirus protection.

Configuring Gateway AntiVirus System Settings

You use the Gateway AntiVirus™ window to enable Gateway AntiVirus and configure Gateway AntiVirus. This window configures the Gateway AntiVirus feature for all SMTP Proxies on the Firebox. You can also create different configurations in each SMTP Proxy. For more information, see “Configuring Gateway AntiVirus in the SMTP Proxy,” on page 9.

Configure Gateway AntiVirus

- 1 In Policy Manager, select **Setup > Gateway AntiVirus**. The **Gateway AntiVirus** dialog box appears.



- 2 If Gateway AntiVirus is not enabled, select the **Enable antivirus engine** check box.
- 3 To temporarily decompress files that are compressed to scan contents for viruses, select the **Temporarily decompress attachments before a scan** checkbox.

This option allows the Firebox to examine the contents of compressed files, for example Zip files, TAR files, and TGZ files.

NOTE

Gateway AntiVirus can only examine one level of a compressed file. Hackers can hide viruses in compressed files that are inside other compressed files. Gateway AntiVirus supports several compression methods. See the Release Notes for this product for a list of the compression file types supported by this release.

- 4 To record debug log messages for Gateway AntiVirus, select the **Enable debug log messages** checkbox.

Use this checkbox to record log messages about the functionality of the antivirus service. It is not usually necessary to record these messages unless the antivirus service does not operate correctly. If this option is selected, log messages are recorded that give more detail about the operation of the antivirus engine. These messages can be used with Tech Support to troubleshoot problems.

- 5 You can set a maximum attachment size to examine in the **Maximum size of file attachments to scan** field.

GatewayAntiVirus allows you to configure the attachment file size from 10 KB to 4096 KB. You can use the arrows to move up or down in 128 KB increments, or type a number between 10 and 4096.

NOTE

Note that this setting does not automatically change the setting in the SMTP Proxy general tab for Maximum Size. The smallest size setting of these two properties takes precedence.

- 6 To get automatic updates to the antivirus engine, select the **Enable automatic AV engine download** checkbox.

Automatic engine updates enable you to have the best antivirus protection available from WatchGuard for the Gateway AntiVirus service.

- 7 To get signature updates automatically, select the **Update automatically** checkbox. Select or type the number of hours between update checks.

Signature updates allow Gateway AntiVirus to protect your system from new virus threats that appear. Set the Firebox to get frequent automatic updates to protect your network better.

Configuring Gateway AntiVirus in the SMTP Proxy

You use Gateway AntiVirus™ to find and stop viruses with the SMTP Proxy. The Firebox uses the SMTP Proxy to examine e-mail messages.

This guide gives you the basic procedure to add an SMTP Proxy, and the procedure for configuring Gateway AntiVirus. For full configuration information for the SMTP Proxy, see your WatchGuard System Manager User Guide.

Add an SMTP Proxy with Gateway AntiVirus

To add an SMTP Proxy and configure Gateway AntiVirus:

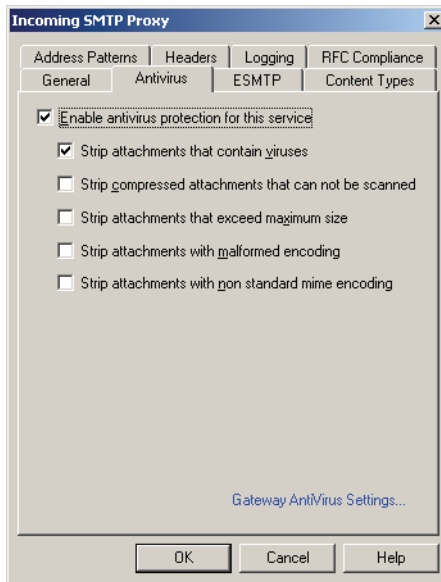
- 1 Start Policy Manager.
- 2 Select **Edit > Add Service**, expand the **Proxies** folder, and select **SMTP**.
- 3 Click **Add**.
- 4 Type a name for the service and click **OK**.

-
- 5 Configure the Incoming and Outgoing connections and traffic configurations for your network.

NOTE

Gateway AntiVirus can be configured for incoming e-mail, outgoing e-mail, or both. You can use these instructions for both incoming and outgoing connections.

- 6 Click the **Properties** tab. Click the **Incoming** or **Outgoing** button. Click the **AntiVirus** tab.
The AntiVirus configuration for this Proxy appears.



- 7 To enable AntiVirus on this Proxy, select the **Enable antivirus protection for this service** check box.
- 8 To remove attachments that contain viruses, select the **Strip attachments that contain viruses** check box.

NOTE

This option is enabled in the default configuration. It is recommended that you use this option. Your users are only protected from viruses if this check box is selected.

- 9 To remove compressed attachments that can not be scanned by Gateway AntiVirus, select the **Strip compressed attachments that can not be scanned** check box.
Compressed attachments that can not be scanned include files that use unsupported compression formats such as RAR 3.0, and password-protected ZIP or other compressed files. This is not enabled by default. It is not recommended that you enable this option.
- 10 To remove attachments that exceed the maximum size, select the **Strip attachments that exceed maximum size** check box.
You can configure the maximum size in the Gateway AntiVirus dialog box. See "Configuring Gateway AntiVirus System Settings" on page 7. This setting is not enabled by default, and it is not recommended that you enable it.
- 11 To remove attachments with malformed encoding, select the **Strip attachments with malformed encoding** check box.
- 12 To remove attachments that are not encoded according to MIME standards, select the **Strip attachments with non standard mime encoding** check box.
Malformed MIME encoding is an exploit that attempts to alter a standard MIME encoding to bypass the content check in Gateway AntiVirus. Non-standard encoding is MIME data that is crafted to appear as correct, but does not adhere to strict standards for the particular MIME encoding. If you enable one or both of these options, those malformed or non-standard MIME object, Gateway AntiVirus strips the MIME object.
- 13 Click **OK**.
The Service Properties window appears.
- 14 When you complete the configuration for the SMTP Proxy, click **OK**.
- 15 Click **OK** to close the **Add Service** dialog box.
- 16 Save the configuration to the Firebox. Select **File > Save > To Firebox**.
- 17 Select a configuration file to save, or type the name of a new file, and click **Save**.
- 18 Type the configuration passphrase in the **Save to Firebox** dialog box.
- 19 Click **Continue** to save the file to the Firebox.

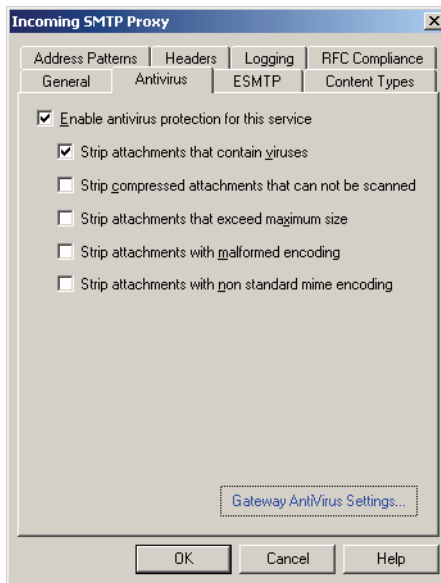
20 Click **OK** after the Firebox is configured.

Configure Gateway AntiVirus for an existing SMTP Proxy

To add Gateway AntiVirus to an existing SMTP Proxy:

- 1 Start Policy Manager.
- 2 Double-click the SMTP Proxy service.
- 3 Click the **Properties** tab. Click the **Incoming** button. Click the **AntiVirus** tab.

The AntiVirus configuration for this Proxy appears.



- 4 To enable AntiVirus on this Proxy, select the **Enable antivirus protection for this service** checkbox.
- 5 To remove attachments that contain viruses, select the **Strip attachments that contain viruses** checkbox.

NOTE

This option is enabled in the default configuration. It is recommended that you use this option. Your users are only protected from viruses if this checkbox is selected.

- 6 To remove compressed attachments that can not be scanned by Gateway AntiVirus, select the **Strip compressed attachments that can not be scanned** checkbox.
Compressed attachments that can not be scanned include files that use unsupported compression formats such as RAR 3.0, and password-protected ZIP or other compressed files. This is not enabled by default. It is not recommended that you enable this option.
- 7 To remove attachments that exceed the maximum size, select the **Strip attachments that exceed maximum size** checkbox.
You can configure the maximum size in the Gateway AntiVirus dialog box. See "Configuring Gateway AntiVirus System Settings" on page 7. This setting is not enabled by default, and it is not recommended that you enable it.
- 8 To remove attachments with malformed encoding, select the **Strip attachments with malformed encoding** checkbox.
- 9 To remove attachments that are not encoded according to MIME standards, select the **Strip attachments with non standard mime encoding** checkbox.
- 10 Malformed MIME encoding is an exploit that attempts to alter a standard MIME encoding to bypass the content check in Gateway AntiVirus. Non-standard encoding is MIME data that is crafted to appear as correct, but does not adhere to strict standards for the particular MIME encoding. If you enable one or both of these options, those malformed or non-standard MIME objects, Gateway AntiVirus strips the MIME object.
- 11 Click **OK**.
The Service Properties window appears.
- 12 When you complete the configuration for the SMTP Proxy, click **OK**.
- 13 Save the configuration to the Firebox. Select **File > Save > To Firebox**.
- 14 Select a configuration file to save, or type the name of a new file, and click **Save**.
- 15 Type the configuration passphrase in the **Save to Firebox** dialog box.
- 16 Click **Continue** to save the file to the Firebox.

17 Click **OK** after the Firebox is configured.

Using Gateway AntiVirus with More Than One Proxy

You can use more than one SMTP Proxy to find and remove viruses for different servers in your organization.

Each proxy that uses Gateway AntiVirus is configured with options that are unique to that proxy. For example, you can use different proxy antivirus configurations for e-mail that is for different servers or different destinations.

Gateway AntiVirus Headers

Gateway AntiVirus adds a header to each e-mail message. An e-mail message can include multiple parts separated by MIME boundaries (multipart MIME). Each MIME part has a separate set of headers. If a part includes an attachment, Gateway AntiVirus adds the header

X-AntiVirus to the set of headers. This header indicates antivirus activity for the part. The X-AntiVirus header indicates whether the message is clean, infected with a virus, or whether there is another error in the antivirus process. If a part includes an attachment, the antivirus action is included in the header. The action can be **allow** or **deny**.

In this example, an attachment is infected with a virus, and the virus is detected by Gateway AntiVirus for E-mail:

```
date time smtp-proxy[signature number]: Attachment
attachment_name is infected with virus virus_name,
denying attachment
```

If an attachment is denied, the body for that part of the message is replaced. The new part is a message similar to the value of the smtp-proxy header, for example:

```
Attachment attachment_name is infected with
virus virus_name, attachment denied
```

Monitoring Gateway AntiVirus Activity

You can monitor Gateway AntiVirus with the logging tools. The Firebox System Manager includes reports and real-time log message monitors.

When Gateway AntiVirus scans an attachment or identifies a virus and removes an attachment, it records a log message in the log file.

These are example Gateway AntiVirus log messages in the Simple Log format:

Message	Meaning
AV: attachment <i>filename</i> is clean Where <i>filename</i> is the name of the file that is scanned	The Firebox scanned an attachment that does not contain a virus.
AV: attachment <i>filename</i> is infected with virus <i>virusname</i> , denying attachment Where <i>filename</i> is the file that is scanned, and <i>virusname</i> is the name of the virus that is detected.	The Firebox scanned an attachment and found a virus. The attachment was removed.
AV: attachment <i>size</i> not scanned due to size, denying attachment	Gateway AntiVirus found a file that exceeds the size limit, and removed it. This occurs when Gateway AntiVirus is configured to strip attachments that exceed the maximum size.

The example below shows a debugging log. In addition to the messages listed above, it includes log messages that describe the operation of each step that Gateway AntiVirus.

```
12/03/04 11:09 smtp-proxy[197]: Entering InitAV
12/03/04 11:09 smtp-proxy[197]: [60.100.253.9:4847 10.9.9.3:25]
removing ESMTTP keyword "PIPELINING"
12/03/04 11:09 smtp-proxy[197]: [60.100.253.9:4847 10.9.9.3:25]
removing ESMTTP keyword "VERFY"
12/03/04 11:09 smtp-proxy[197]: [60.100.253.9:4847 10.9.9.3:25]
removing ESMTTP keyword "ETRN"
12/03/04 11:09 smtp-proxy[197]: [60.100.253.9:4847 10.9.9.3:25]
removing ESMTTP keyword "XVERP"
12/03/04 11:09 smtp-proxy[197]: AV: attachment avnormal.txt will be
scanned
12/03/04 11:09 avd[138]: Accepted client on 10
12/03/04 11:09 smtp-proxy[197]: AV: received response, response is /
tmp/clamav/s0 4096
```

```
12/03/04 11:09 smtp-proxy[197]: AV: socket setup complete
12/03/04 11:09 smtp-proxy[197]: AV: entering AVCleanSpace
12/03/04 11:09 smtp-proxy[197]: AV: scan file path /tmp/clamav/s0/
1197, av state 0, max file size 4194304
12/03/04 11:09 smtp-proxy[197]: AV: attachment encoding is base64
12/03/04 11:09 smtp-proxy[197]: AV: write to disk complete, bytes
written 33537
12/03/04 11:09 smtp-proxy[197]: AV: scan command is "scan default 197 /
tmp/clamav/s0/1197"
12/03/04 11:09 smtp-proxy[197]: AV: scan response is "clean 197"
12/03/04 11:09 smtp-proxy[197]: AV: attachment avnormal.txt is clean
12/03/04 11:09 smtp-proxy[197]: mail from address
<user@watchguard.com>
12/03/04 11:09 smtp-proxy[197]: rcpt to address
<user2@watchguard.com>
12/03/04 11:09 smtp-proxy[197]: AV: base64 encode attachment
12/03/04 11:09 smtp-proxy[197]: AV: attachment read from disk (33537)
and written to socket (46071)
12/03/04 11:09 smtp-proxy[197]: AV: antivirus scan done
12/03/04 11:09 smtp-proxy[197]: AV: entering AVCleanSpace
12/03/04 11:09 smtp-proxy[197]: AV: attachment avviral.txt will be
scanned
12/03/04 11:09 smtp-proxy[197]: AV: scan file path /tmp/clamav/s0/
2197, av state 0, max file size 4194304
12/03/04 11:09 smtp-proxy[197]: AV: attachment encoding is base64
12/03/04 11:09 smtp-proxy[197]: AV: write to disk complete, bytes
written 68
12/03/04 11:09 smtp-proxy[197]: AV: scan command is "scan default 197 /
tmp/clamav/s0/2197"
12/03/04 11:09 smtp-proxy[197]: AV: scan response is "virus 197 Eicar-
Test-Signature"
12/03/04 11:09 smtp-proxy[197]: AV: antivirus action is deny
12/03/04 11:09 smtp-proxy[197]: AV: attachment avviral.txt is infected
with virus Eicar-Test-Signature, denying attachment
12/03/04 11:09 smtp-proxy[197]: mail from address
<user@watchguard.com>
12/03/04 11:09 smtp-proxy[197]: rcpt to address
<user2@watchguard.com>
12/03/04 11:09 smtp-proxy[197]: AV: antivirus scan done
12/03/04 11:09 smtp-proxy[197]: AV: entering AVCleanSpace
```