Writing a virus sample to file for McAfee Labs submission

(For Web Gateway 7.2 and later)

Contents

History

Revision	Date	Description
A	May 25, 2012	Initial release
B	June 13, 2012	Updated instructions to reference Online RuleSet Library

Overview

This document outlines the process for which a Web Gateway administrator can utilize the Web Gateway to capture virus information, and direct it to a file for submission to the McAfee Labs team. This document only covers information for capturing False positives, not False negatives.

For more information see the original KB article discussing the submission process, How to submit virus and anti-malware samples for analysis -- False Positives or False Negatives: KB62662, https://kc.mcafee.com/corporate/index?page=content&id=KB62662.

Prerequisites

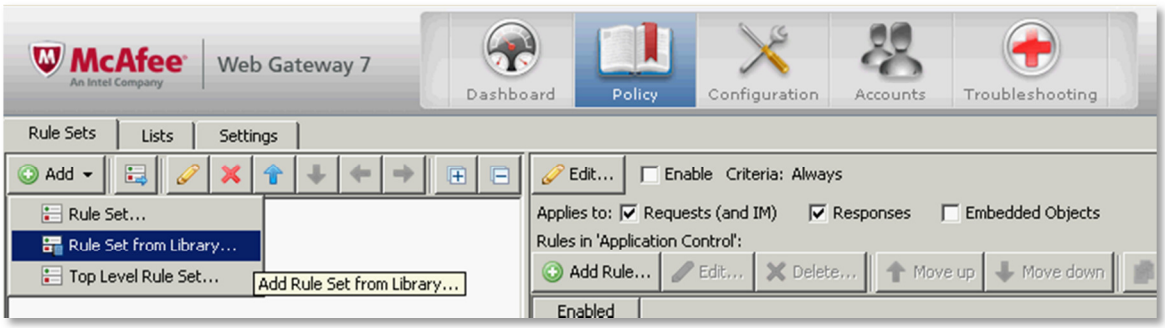
In order for you to successfully complete the steps outlined in this document you will need the following:

- Access to the Web Gateway GUI interface
- Command line access (to safely collect and compress the virus sample).

Importing the "Write Virus Samples to Files" RuleSet

To start you must download, extract, and import a RuleSet for which we will use to collect a virus sample.

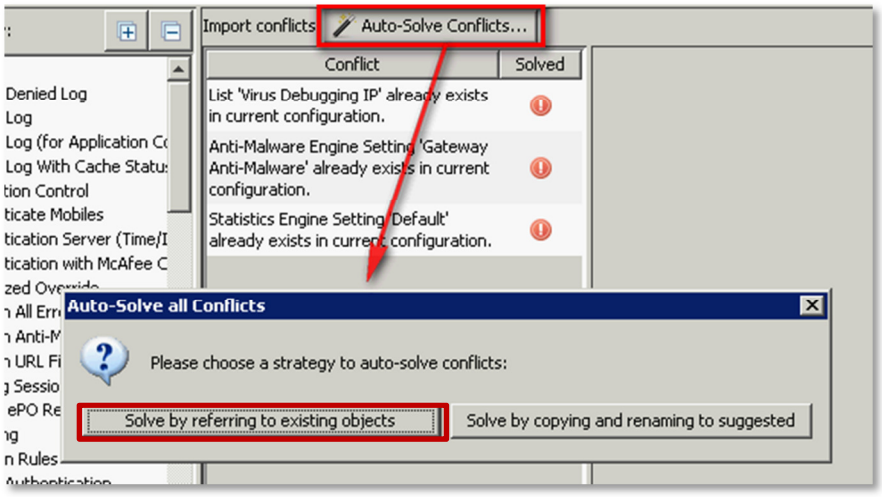
1. Open the "Rule Set from Library" dialog:



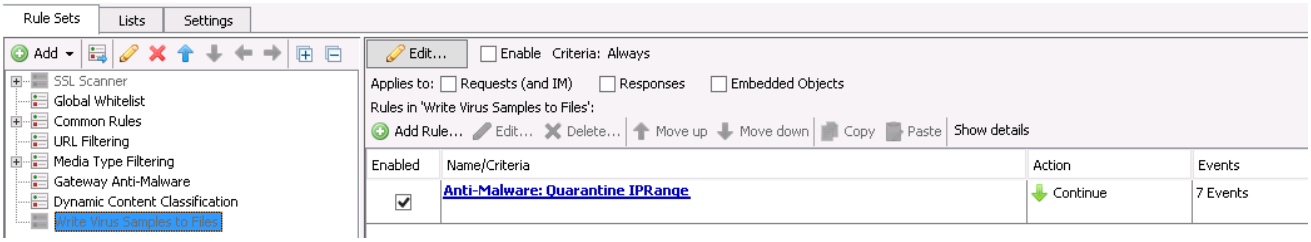
2. Go to the Online RuleSet Library to download the “Write Virus Samples to Files” RuleSet (search for "Virus"):

Online Rule Library:

3. Once the RuleSet has been downloaded and extracted, navigate back to the RuleSet Library, and choose the option to "Import from File" and browse for the downloaded file. Choose "Auto-solve conflict…Solve by referring to existing objects":



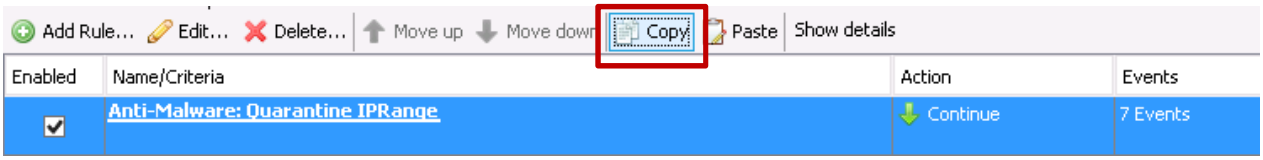
Below is the imported, but disabled, RuleSet:



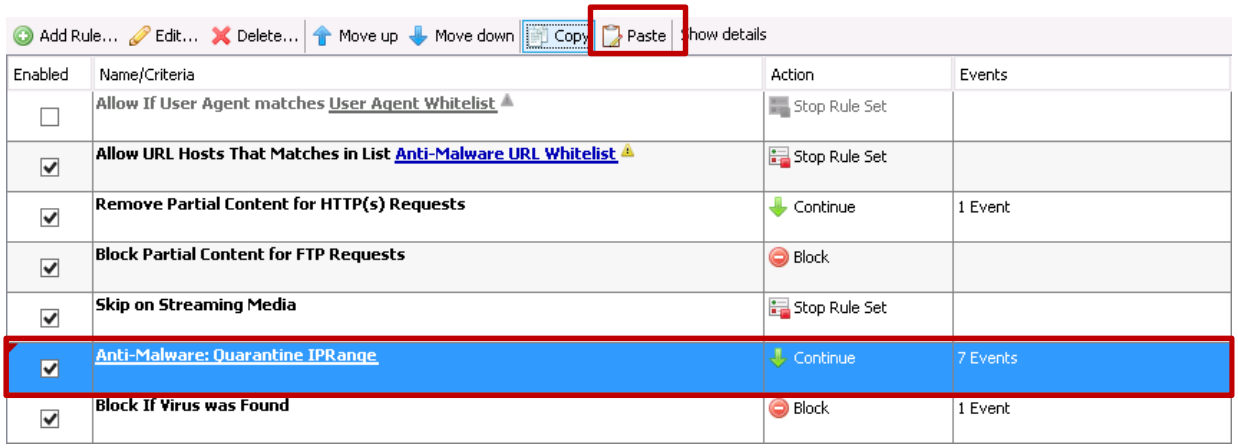
Modify rule placement and criteria

Once the RuleSet has been imported the rule must be copied, placed within the existing "Gateway Anti-Malware" RuleSet, and a client IP address must be added to the list referenced in the rule.

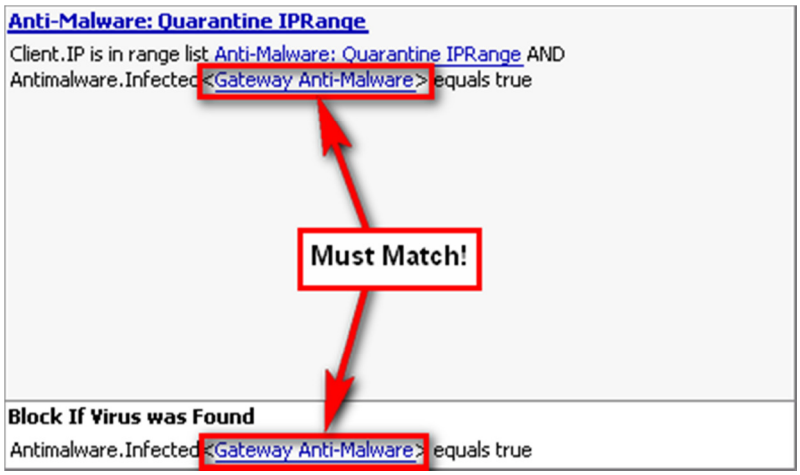
1. Select the "Anti-Malware: Quarantine IP Range" rule and click copy:



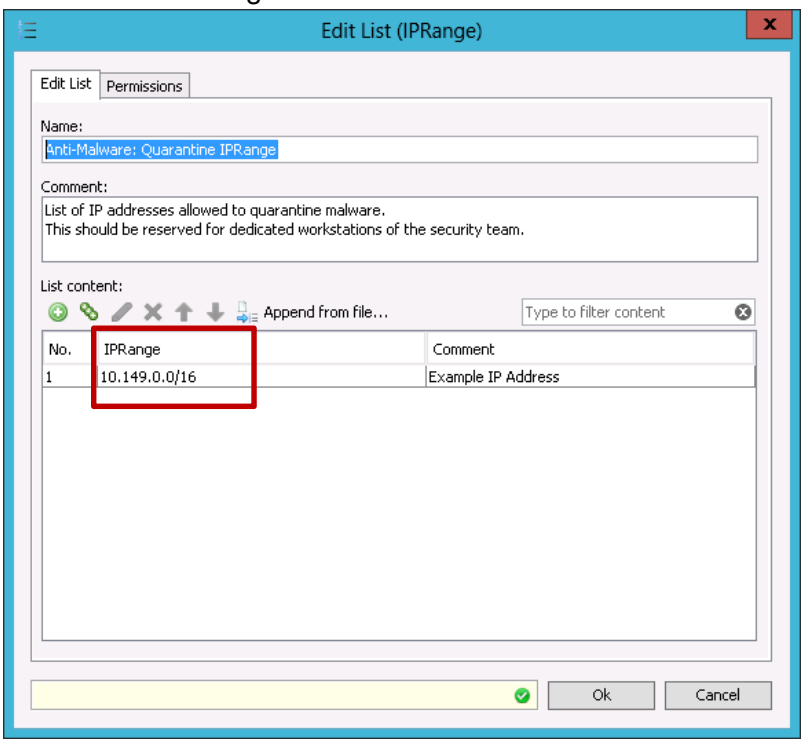
2. Paste the rule into your existing "Gateway Anti-Malware" RuleSet, placing it just above the "Block if Virus was Found":



3. The engine settings for the rules must match:



4. Next, add a client IP address to the "Anti-Malware: Quarantine IP Range" list within the "Anti-Malware: Quarantine IP Range" rule. This is the client IP address from which you'll recreate the virus block:



Recreate the Virus block

In order for a sample to be created, you must recreate the virus block with the new rules in place.

1. Reproduce the false positive detection from the same client IP address entered in the prior step:

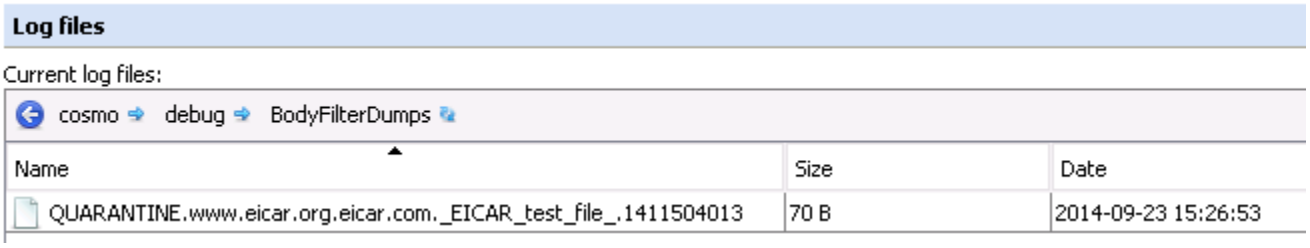
***Make note of the Virus Name displayed on the block page. This info is used later when the sample is submitted via KB62662.

2. Once the detection is reproduced, a virus sample is written to a file for collection.

Collect the sample

To collect the sample in a secure manner it is recommended to login to the CLI of the appliance. From the CLI, compress and encrypt the file using the steps below.

1. The file is available from the GUI, but to safely handle the file, we should compress and encrypt it first.



2. Open putty or any other SSH tool and login to the appliance.
3. Move to the /opt/mwg/log/debug/BodyFilterDumps directory:

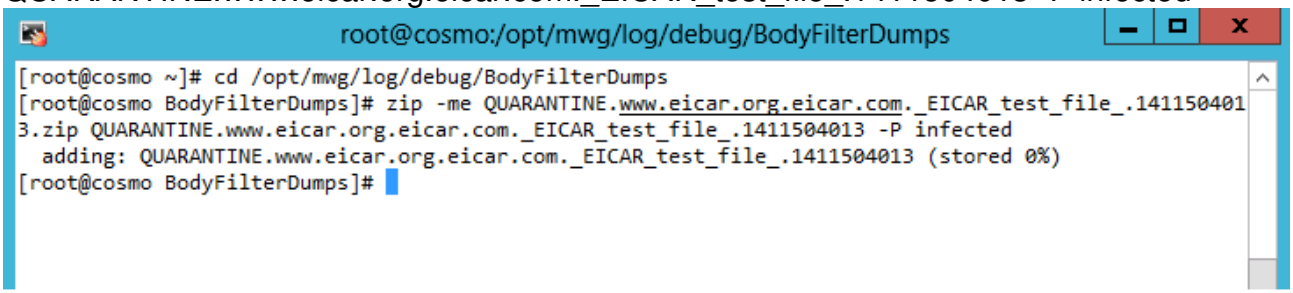
   cd /opt/mwg/log/debug/BodyFilterDumps

4. Compress and encrypt the file using the following command (**password must be "infected"**):

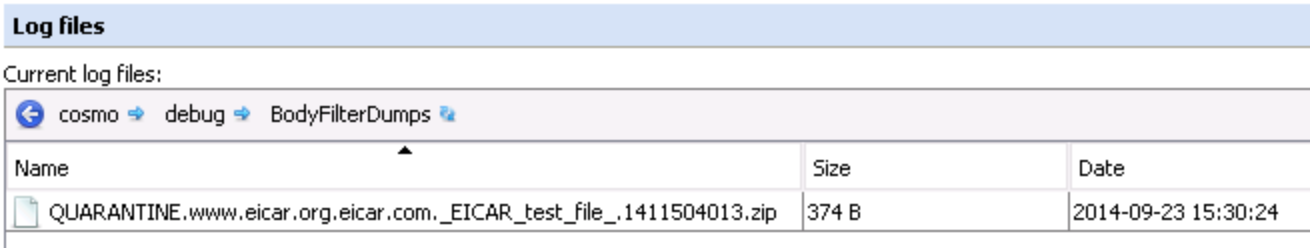
   zip -me <FILENAME>.zip <FILENAME> -P infected

   # EXAMPLE:

   zip -me QUARANTINE.www.eicar.org.eicar.com._EICAR_test_file_.1411504013.zip QUARANTINE.www.eicar.org.eicar.com._EICAR_test_file_.1411504013 -P infected



5. You can now safely download the compressed and encrypted file from the GUI:



Submission process

Refer to KB62662, https://kc.mcafee.com/corporate/index?page=content&id=KB62662, for submitting the sample to McAfee Labs.

As the Web Gateway supports multiple Anti-Virus/Anti-Malware engines, please ensure you follow the steps for the respective virus engine which was noted on the virus block page. Below is a list of the example virus names, each are prefaced with their respective engine name:

- VirusName: "**McAfeeGW:** EICAR test file", *follow the **"McAfee Gateway Anti-Malware"** submission steps in KB62662.*
- VirusName: "**McAfee:** EICAR test file", *follow the **"McAfee AV"** submission steps in KB62662.*
- VirusName: "**Avira:** Eicar-Test-Signature", *follow the **"AVIRA"** submission steps in KB62662.*