Application Firewall Pack (AFP)

Feature Description

VERSION: 1.8

UPDATED: MARCH 2015

Copyright Notices

Table of Contents

1 Introduction

Application Firewall Pack (AFP) services enable natively integrated Web Application Firewall (WAF) protection in the KEMP LoadMaster. This enables secure deployment of web applications, preventing Layer 7 attacks while maintaining core load balancing services which ensures comprehensive application delivery and security. AFP functionality directly augments the LoadMaster's existing security features to create a layered defence for web applications - enabling a safe, compliant and productive use of published services.

For a more detailed overview of the AFP feature, please refer to the AFP section in the **KEMP LoadMaster, Product Overview**.

1.1 Document Purpose

The purpose of this document is to describe the AFP features and provide step-by-step instructions on how to configure the AFP settings in the KEMP LoadMaster.

For further information and assistance, please refer to our KEMP Support site which Support contact details: http://kemptechnologies.com/load-balancing-support/kemp-support/.

1.2 Intended Audience

This document is intended to be read by anyone who is interested in finding out more about the KEMP AFP functionality.

2 Configuring AFP

2.1 Resource Considerations

> Utilizing AFP can have a significant performance impact on the LoadMaster deployment. Please ensure that the appropriate resources are allocated.

For virtual and bare metal LoadMaster instances, a minimum of 2GB of allocated RAM is required for operation of AFP. The default memory allocation for Virtual LoadMasters and LoadMaster Bare Metal instances prior to LoadMaster Operating System version 7.1-22 is 1GB of RAM. If this default allocation has not been changed please modify the memory settings before attempting to proceed with AFP configuration.

2.2 AFP Rule Management

If you have an AFP license and AFP Support, KEMP provides a number of commercial rules, such as **ip_reputation**, which can be set to automatically download and update on a daily basis. These commercial rules are targeted to protect against specific threats that packaged and custom applications are vulnerable to. The KEMP-provided commercial rules are available when signed up to an AFP subscription.

You can also upload other rules such as the ModSecurity core rule set which contains generic attack detection rules that provide a base level of protection for any web application.

You can also write and upload your own custom rules, if required.

With the AFP-enabled LoadMaster, you can choose whether to use KEMP-provided rules, custom rules which can be uploaded or a combination of both. The sections below provide details regarding commercial rules and custom rules.

> Microsoft Exchange 2010 and Exchange 2013 Remote Procedure Call (RPC) requests will fail if AFP is enabled because the AFP rules do not support the RPC methods.

2.2.1 Commercial Rules

The KEMP-provided commercial rules can be set to automatically download and install, if desired. They can also be manually downloaded and installed. The sections below explain how to use each method.

> KEMP-provided commercial rules are only available when signed up for an AFP subscription.

2.2.1.1 Automatic Downloading and Updating of Commercial Rules

Follow the steps below to configure automatic download and installation settings for WAF commercial rules:

1. In the main menu, select **Virtual Services > WAF Settings**.

Figure 2-1: WAF Rule Management

2. To enable the automatic download of updates to AFP commercial rule files, select the **Enable Automated Rule Updates** check box.

> The automatic and manual download options will be greyed out if AFP support has expired. If this is the case, please contact KEMP to renew your subscription if desired.

3. To enable automatic installation of the updated AFP commercial rule files, select the **Enable Automated Installs** check box.

> By default, the **Enable Automated Installs** and **Manually Install rules** options are greyed out. The rules need to be downloaded for the first time before these options become available.

4. Select the time (hour of the day) at which to automatically install the commercial rule updates.

> The AFP rules must be assigned to a Virtual Service in order to take effect. For instructions on how to assign AFP rules to a Virtual Service, refer to **Section 2.3**.

2.2.1.2 Manual Downloading and Updating of Commercial Rules

To manually download and install the commercial rule file updates, follow the steps below:

1. In the main menu, select Virtual Services > WAF Settings.

Figure 2-2: WAF Rule Management

2. Click the **Download Now** button to attempt to download the AFP rules now.

> A warning message will appear here if the rules have not been updated in the last 7 days, or if they have not been downloaded at all.

3. Click the **Install Now** button to manually install the commercial rule updates.

> The AFP rules must be assigned to a Virtual Service in order to take effect. For instructions on how to assign AFP rules to a Virtual Service, refer to **Section 2.3**.

2.2.2 Custom Rules

Third party rules, such as the ModSecurity core rule set can be uploaded to the LoadMaster, if required. You can also write your own custom rules which can be uploaded, if needed. The **WAF Rule Management** screen allows you to upload **Custom Rules** (.conf) and associated **Custom Rule Data** (.data or .txt) files. You can also upload Tarball files (.tar.gz) which contain multiple rule and data files.

To upload rule and data files, follow the steps below:

1. In the main menu, select **Virtual Services > WAF Settings**.

Figure 2-3: WAF Rule Management

2. To upload custom rules, click **Choose File** in the **Installed Rules** section.

> Individual rules can be uploaded as .conf files. Alternatively, you can load a package of rules in a tar.gz file, for example the ModSecurity core rule set.

3. Browse to and select the rule file(s) to be uploaded.
4. Click **Add Ruleset**.
5. To upload any additional data files, click **Choose File** in the **Custom Rule Data** section.

> The additional files are for the rules' associated data files. If you uploaded a Tarball in **Step 3**, the rules and data files can be packaged together.

6. Browse to and select the additional data files to be uploaded.
7. Click **Add Data File**.

The rules will now be available to assign within the Virtual Services modify screen. Refer to the next section to find out how to configure the Virtual Service to use the installed rules (commercial or custom).

2.3 Configure AFP Options for a Virtual Service

AFP settings can be configured for each individual Virtual Service. Follow the steps below to configure the AFP options in a Virtual Service. For more information on each of the fields, refer to **Section 2.4**.

1. In the main menu of the LoadMaster WUI, select **Virtual Services > View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. Expand the **WAF Options** section.

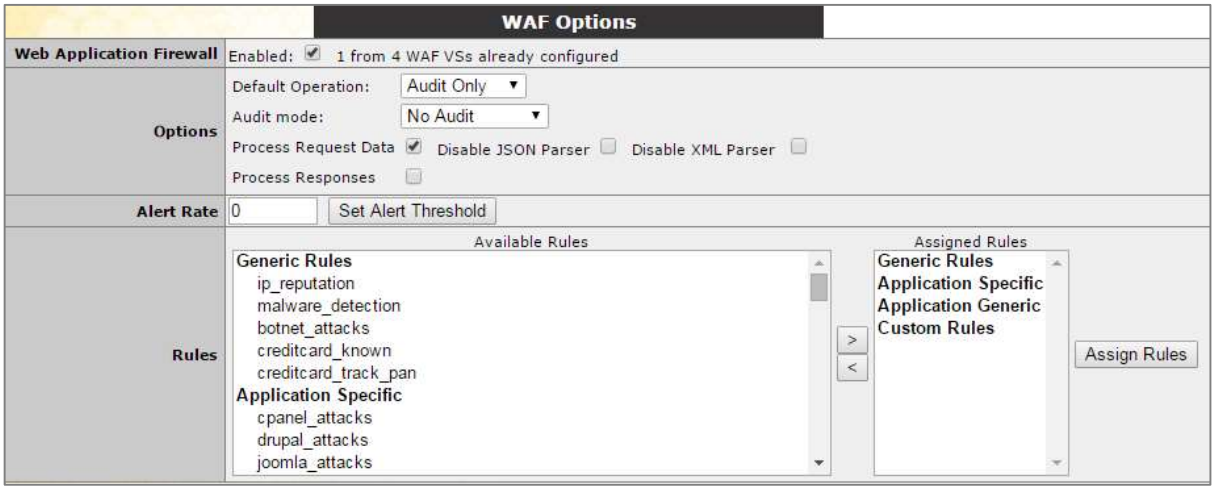

Figure 2-4: WAF Options

4. By default, AFP is disabled. To enable AFP, select **Enabled**.

The maximum number of AFP-enabled Virtual Services is the total RAM/512 MB, for example 8 GB/512 MB = 16 AFP Virtual Services. When the maximum is reached, no additional Virtual Services can be enabled with AFP.

A message will be displayed next to the **Enabled** check box displaying how many WAF-enabled Virtual Services exist and it will also display the maximum number of WAF-enabled Virtual Services that can exist. If the maximum number of WAF-enabled Virtual Services have been reached, the **Enabled** check box will be greyed out.

5. Specify the **Default Operation** type.

The **Default Operation** is what will occur if no action is specified in the relevant rule.

Audit Only: This is an audit-only mode – logs will be created but requests and responses are not blocked.

Block Mode: Either requests or responses are blocked based on the assigned rules.

6. Specify the **Audit mode**.

There are three audit modes:

No Audit: No data is logged.

Audit Relevant: Logs data which is of a warning level and higher.

Audit All: Logs all data through the Virtual Service.

Selecting the **Audit All** option produces a large amount of log data. KEMP does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

7. Specify whether or not to **Process Request Data**.

The **Process Request Data** option is disabled by default. If you enable the Process Request Data option, two more check boxes become available which allow you to disable the processing of JavaScript Object Notation (JSON) and XML requests.

8. Specify whether or not to **Process Responses**.

The processing of response data can be CPU and memory intensive.

9. Specify the **Alert Rate** and click **Set Alert Threshold**.

This is the number of incidents per hour before sending an alert. Setting this to **0** disables alerting.

10. Assign rules by selecting them in the **Available Rules** section and clicking the right arrow to move them into the **Assigned Rules** section. Then, click **Assign Rules**.

Application-specific and application-generic rules cannot both be assigned to the same Virtual Service. If you try to do this, an error message (**Cannot assign Application Specific and Application Generic rules simultaneously**) will appear to inform you that this is not possible.

2.4 Backing Up and Restoring an AFP Configuration

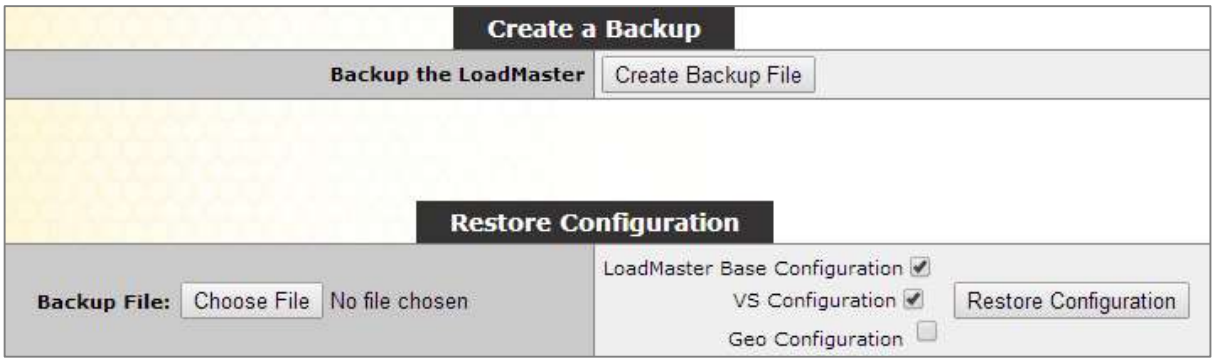

Figure 2-5: Back Up and Restore

A backup of the LoadMaster configuration can be taken by going to **System Administration > Backup/Restore** and clicking **Create Backup File**.

The configuration can be restored from this screen also. Please keep in mind that the Virtual Service settings can be restored by selecting **VS Configuration** and the rules can be restored by selecting **LoadMaster Base Configuration**.

> An AFP configuration can only be restored onto a LoadMaster with an AFP license.

2.5 AFP WUI Options

This section describes the different AFP fields available in the LoadMaster WUI. There are AFP WUI options in the **WAF Settings** section of the main menu and in the Virtual Service modify screen. Refer to the sections below for field descriptions.

2.5.1 WAF Settings in the Main Menu of the LoadMaster WUI

You can get to this screen by selecting **Virtual Services > WAF Settings** in the main menu of the LoadMaster WUI.

Figure 2-6: WAF Rule Management

This is the WAF Rule Management screen.

> The automatic and manual download options will be greyed out if the AFP subscription has expired.

Enable Automated Rule Updates

Select this check box to enable the automatic download of the latest AFP rule files. This is done on a daily basis, if enabled.

Last Updated

This section displays the date when the last rules were downloaded. It gives you the option to attempt to download the rules now. It will also display a warning if rules have not been downloaded in the last 7 days.

Enable Automated Installs

Select this check box to enable the automatic daily install of updated rules at the specified time.

When to Install

Select the hour at which to install the updates every day.

Manually Install rules

This button allows you to manually install rule updates, rather than automatically installing them. This section also displays when the rules were last installed.

Custom Rules

This section allows you to upload custom rules and associated data files. Individual rules can be loaded as .conf files, or you can load a package of rules in a Tarball (tar.gz) file.

Custom Rule Data

This section allows you to upload data files which are associated to the custom rules.

WAF Options in the Virtual Service Modify Screen

You can get to the Virtual Service AFP Options by selecting **Virtual Services > View/Modify Services** in the main menu, clicking **Modify** on the relevant Virtual Service and expanding the **WAF Options** section.

Figure 2-7: Enable WAF

By default, WAF is disabled. To enable AFP, select the **Enabled** check box.

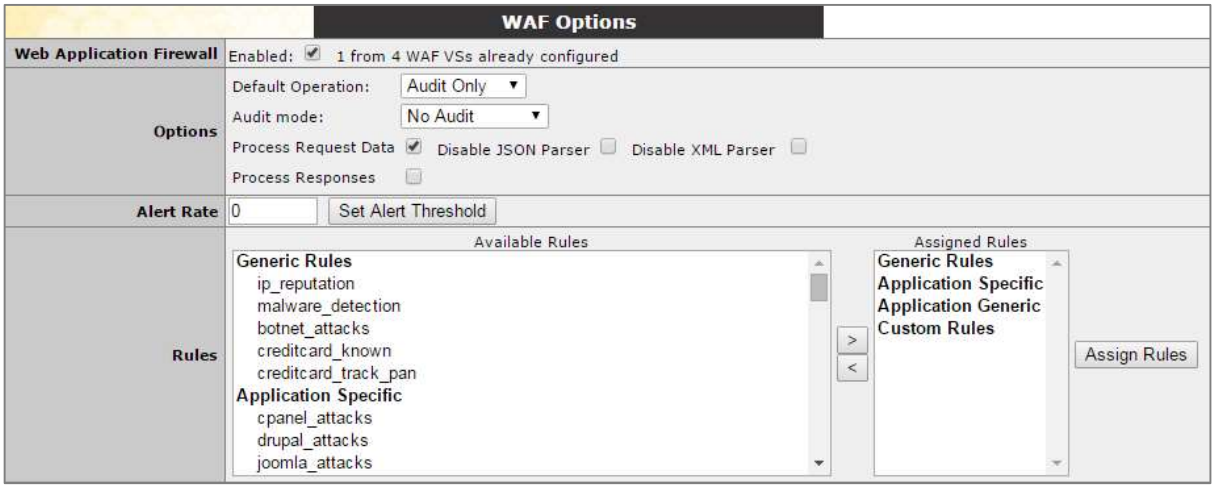

Figure 2-8: WAF Options (per Virtual Service)

The AFP feature must be enabled before you can configure these options. Select the **Enabled** check box to enable AFP on this Virtual Service.

Default Operation

Specify the Default Operation type:

- **Audit Only:** This is an audit-only mode – logs will be created but requests and responses are not blocked.
- **Block Mode:** Either requests or responses are blocked based on the assigned rules.

Audit mode

Audit logs are produced according to the specifications on the following website:
https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-2-Data-Formats

Select what logs to record:

- **No Audit:** No data is logged.
- **Audit Relevant:** Logs data which is of a warning level and higher.
- **Audit All:** Logs all data through the Virtual Service.

> Selecting the **Audit All** option produces a large amount of log data. KEMP does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

Process Request Data

Enable this option to also process the data supplied in POST requests.

> The **Process Request Data** option is disabled by default. Two additional options (**Disable JSON Parser** and **Disable XML Parser**) only become available if **Process Request Data** is enabled.

Disable JSON Parser

Disable processing of JavaScript Object Notation (JSON) requests.

Disable XML Parser

Disable processing of Extensible Markup Language (XML) requests.

Process Responses

Enable this option to verify response data sent from the Real Servers.

> This can be CPU and memory intensive.

If a Real Server is gzip encoding, WAF will not check that traffic, even if **Process Responses** is enabled.

Alert Rate

This is the threshold of incidents per hour before sending an alert email. Setting this to **0** disables alerting.

Rules

This is where you can assign/un-assign generic, custom, application-specific and application-generic rules to/from the Virtual Service.

Application-specific and application-generic rules cannot both be assigned to the same Virtual Service. If you try to do this, an error message will appear to inform you that this is not possible.

2.5.2 WAF Options in the Extended Log Files Screen

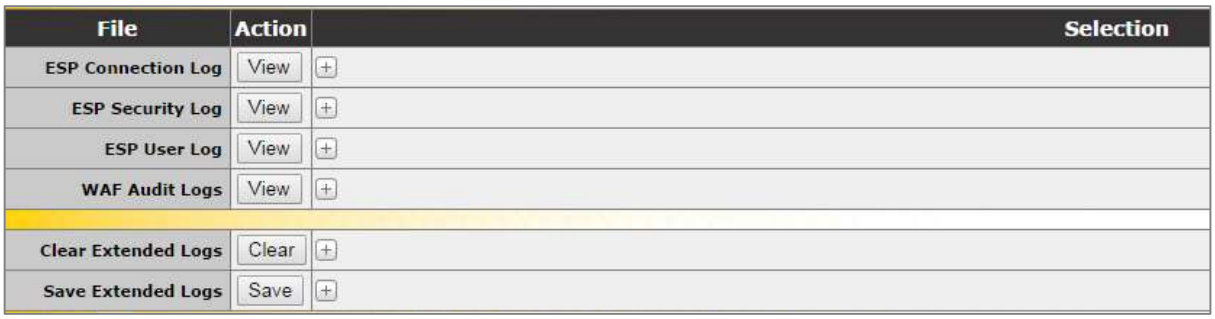

Figure 2-9: Extended Log Files

The **Extended Log Files** screen provides options for logs relating to the ESP and AFP features. These logs are persistent and will be available after a LoadMaster reboot. To view all of the options click on the ⊞ icons.

The AFP logs are not generated in real time – they can be up to two minutes behind what the AFP engine is actually processing.

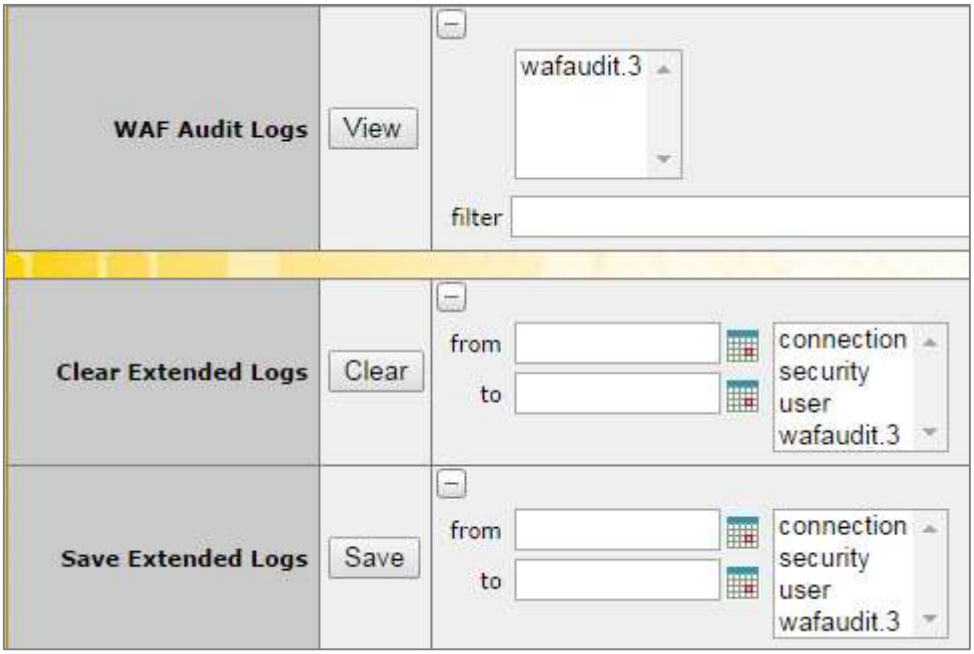

Figure 2-10: Extended Log Files

In addition to AFP logs, ESP logs are also available on this screen. For more information, refer to the **Edge Security Pack (ESP), Feature Description**.

WAF Audit Logs: recording AFP logs based on what has been selected for the **Audit mode** drop-down list (either **Audit Relevant** or **Audit** All) in the **WAF Options** section of the Virtual Service modify screen.

To view the logs please select the appropriate log file and click the relevant **View** button.

The number listed in each log entry corresponds to the ID of the Virtual Service. To get the Virtual Service ID, first ensure that the API interface is enabled (**System Configuration > Miscellaneous Options > Remote Access > Enable API Interface**). Then, in a web browser address bar, enter **https://<LoadMasterIPAddress>/access/listvs**. Check the **index** of the Virtual Service. This is the number that corresponds to the number on the audit log entry.

One or more archived log files can be viewed by selecting the relevant file(s) from the list of file names and clicking the **View** button. You can filter the log files by entering a word(s) or regular expression in the **filter** field and clicking on the **View** field.

Clear Extended Logs

All extended logs can be deleted by clicking the **Clear** button.

Specific log files can be deleted by filtering on a specific date range, selecting one or more individual log files in the log file list or selecting a specific log type (for example connection, security or user) in the log file list and clicking the **Clear** button. Click **OK** on any warning messages.

Save Extended Logs

All extended logs can be saved to a file by clicking the **Save** button.

Specific log files can be saved by filtering on a specific date range, selecting one or more individual log files in the log file list or selecting a specific log type (for example connection, security or user) in the log file list and clicking the **Save** button.

2.5.3 Enable WAF Debug Logging

AFP debug traces can be enabled by clicking the **Enable Logging** button at **System Configuration > Logging Options > System Log Files**.

> This generates a lot of log traffic. It also slows down AFP processing. Only enable this option when requested to do so by KEMP Technical Support. KEMP does not recommend enabling this option in a production environment.
>
> The AFP debug logs are never closed and they are rotated if they get too large. AFP (in general) needs to be disabled and re-enabled (by unticking and re-ticking the **Enabled** check box) in all AFP-enabled Virtual Service settings in order to re-enable the debug logs. Alternatively, perform a rule update (in the **WAF Settings** screen), with rules that are relevant for the Virtual Service(s).

2.5.4 WAF Statistics

2.5.4.1 Home Page

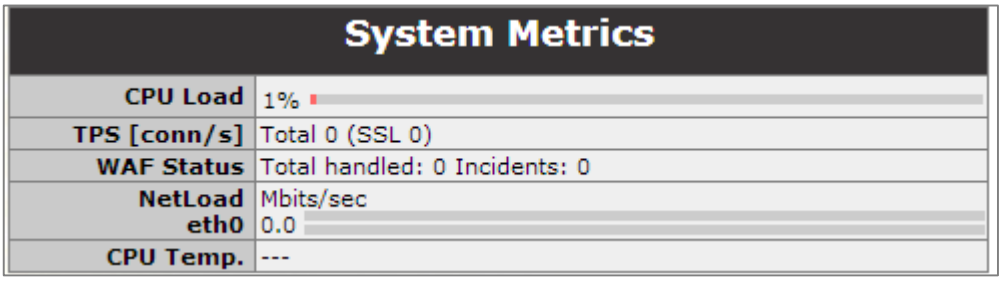

Figure 2-11: System Metrics

On the **Home** page of the LoadMaster WUI, there is a **WAF Status** entry in the **System Metrics** section. This displays the total number of handled connections over all AFP-enabled Virtual Services. It also displays the total number of incidents.

2.5.4.2 Statistics Page

VIP Nickname1	
Address	10.154.60.63
Port	80
Protocol	tcp
Active Conns	0
Total Conns	0
Total Bytes	0
Real Servers	0
Persist Entries	0
WAF	Enabled
Incidents	0

Figure 2-12: Virtual Service AFP statistics

In the **Statistics** page, click **Virtual Services** and then click the **Virtual IP Address** link to see the AFP statistics for that Virtual Service. This screen shows if AFP is enabled or disabled for this Virtual Service. It also displays the number of **Incidents** for the Virtual Service.

2.5.5 WAF Misconfigured Virtual Service Status

Figure 2-13: WAF Misconfigured status

On the **View/Modify Services** screen in the LoadMaster WUI, the **Status** of each Virtual Service is displayed. If the AFP for a particular Virtual Service is misconfigured, for example if there is an issue with a rule file, the status changes to **WAF Misconfigured** and turns to red.

If the Virtual Service is in this state, all traffic is blocked.

AFP can be disabled for that Virtual Service to stop the traffic being blocked, if required, while troubleshooting the problem.

3 Troubleshooting

When uploading a large amount of data, the Real Server will not receive any data until all of the data has been received by the WAF engine. If a large amount of data is being uploaded to the LoadMaster, the Real Servers may close the connection because they have a standard timeout of 15 seconds between opening and receiving data. This results in the following error message:

"The connection was reset : The connection to the server was reset while the page was loading."

References

Unless otherwise specified, the following documents can be found at http://www.kemptechnologies.com/documentation

Edge Security Pack (ESP), Feature Description

KEMP LoadMaster, Product Overview

Web User Interface (WUI), Configuration Guide

Document History

Date	Change	Reason for Change	Version	Resp.
Sep 2014	Initial draft	First draft of document	1.0	LB
Sep 2014	Minor updates	Additional information added	1.1	LB
Oct 2014	Minor updates	Defects resolved	1.2	LB
Nov 2014	Minor updates	Defects resolved	1.3	LB
Nov 2014	Minor updates	Defects resolved	1.4	LB
Dec 2014	Minor updates	Defects resolved	1.5	LB
Jan 2015	Release updates	Updates for 7.1-24 release	1.6	LB
Feb 2015	Minor update	Enhancement made	1.7	LB
Mar 2015	Minor update	Enhancement made	1.8	LB

