Progress®
Kemp® LoadMaster®

Technical Note WAF Rule Writing Guide

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Document Purpose 6

Intended Audience 6

Chapter 2: ModSecurity Rule Writing 7

Variables 8

Operator 9

Transformation Functions 9

Actions 9

Rule Syntax 10

Rule Example 1 – Cross Site Scripting (XSS) Attack 10

Rule Example 2 – Whitelist IP Address 12

Rule Example 3 – Chaining Rules 13

Rule Example 4 – Shellshock Bash Attack 14

WUI Settings 18

Rule Block Function 19

Chapter 3: Managing Custom WAF Rules in the LoadMaster 21

Add a Custom Rule 21

Delete/Download a Custom Rule or Data File 23

Chapter 4: Assigning Custom Rules to a Virtual Service 24

WAF Misconfigured State 26

Chapter 5: Backing Up and Restoring WAF Configuration 27

Chapter 6: References 29

1

Introduction

Introduction

Web Application Firewall (WAF) services are natively integrated in the LoadMaster. This enables secure deployment of web applications, preventing Layer 7 attacks while maintaining core load balancing services which ensures superior application delivery and security. WAF 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.

If you have a WAF license and WAF Support, Progress Kemp provides a number of commercial rules, such as **ip_reputation**. These commercial rules are targeted to protect against specific threats. The Progress Kemp-provided commercial rules are available when signed up to a WAF 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 WAF-enabled LoadMaster, you can choose whether to use Progress Kemp-provided rules, custom rules which can be uploaded or a combination of both.

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

For instructions on how to configure the various WAF options in the LoadMaster, refer to the Web Application Firewall, Feature Description.

Related Links

- Document Purpose
- Intended Audience

Document Purpose

Document Purpose

The purpose of this document is to provide some guidance on how to write your own custom WAF rules. These custom rules can be uploaded to the LoadMaster and assigned to Virtual Services as needed.

Intended Audience

Intended Audience

This document is intended to be read by anyone who is interested in finding out more about how to write custom WAF rules.

2

ModSecurity Rule Writing

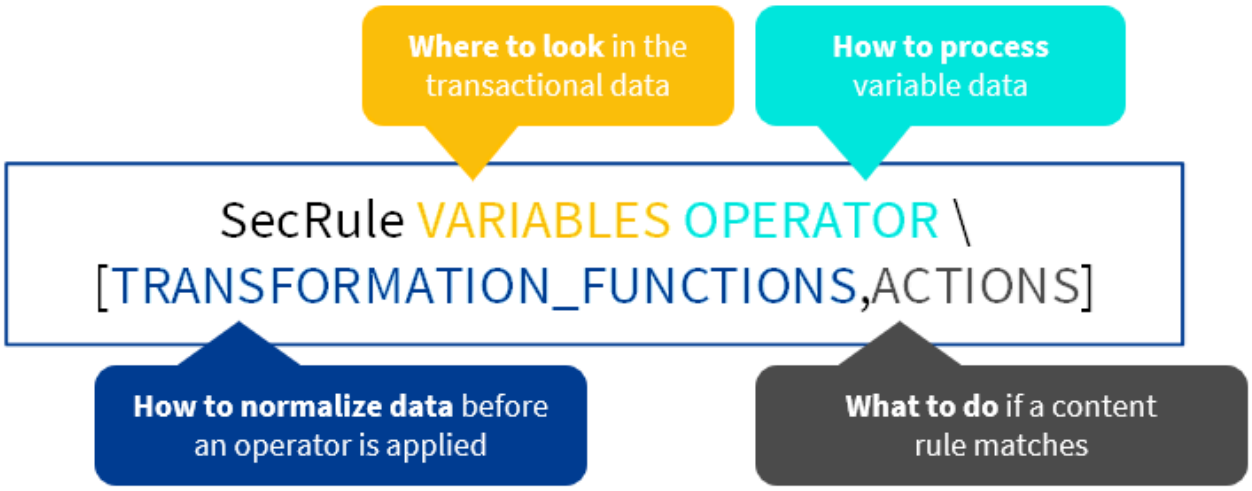
ModSecurity Rule Writing

The ModSecurity Reference Manual should be consulted in any cases where questions arise relating to the syntax of commands: https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual

In terms of rule writing, the main directive to know is SecRule, which is used to create rules and thus does most of the work.

Every rule defined by SecRule conforms to the same format, as below:

```
SecRule VARIABLES OPERATOR \ [TRANSFORMATION_FUNCTIONS,ACTIONS]
```



The rule consists of four parts:

- **VARIABLES:** Tells the WAF engine where to look in the transactional data.
- **OPERATOR:** Tells the WAF engine how to process the variable data.
- **TRANSFORMATION_FUNCTIONS:** Tells the WAF engine how to normalize data before an operator is applied.
- **ACTIONS:** Tells the WAF engine what to do if a rule matches.

The four parts are explained in the sections below.

Related Links

- Variables
- Operator
- Transformation Functions
- Actions
- Rule Syntax
- WUI Settings
- Rule Block Function

Variables

Variables

This specifies which places to check in a HTTP transaction. Examples of variables include:

- **ARGS** – all arguments including the POST payload
- **REQUEST_METHOD** – request method used in the transaction
- **REQUEST_HEADERS** – can be used as either a collection of all of the request headers or can be used

to inspect selected headers

- Etc. The full list of variables is available here: https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#Variables

Operator

Operator

This specifies a regular expression, pattern or keyword to be checked in the variable(s). Operators begin with the @ character. The full list of operators is available here: https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#Operators

Transformation Functions

Transformation Functions

There are a number of transformation functions that can be performed, for example:

- Anti-evasion (such as lowercase, normalisePath, removeNulls, replaceComments, compressWhitespace)
- Decoding (such as base64Decode, hexDecode, jsDecode, urlDecodeUni)
- Encoding (such as base64Encode, hexEncode)
- Hashing (such as sha1, md5)

Actions

Actions

This specifies what to do if the rule matches. Actions are defined in seven categories, listed below:

- **Disruptive** – used to allow ModSecurity to take an action, for example allow or block
- **Flow** – affect the flow, for example skip
- **Meta-data** – used to provide more information about rules
- **Variable** – used to set, change and remove variables
- **Logging** – used to influence the way logging takes place
- **Special** – used to provide access to another class of functionality
- **Miscellaneous** – contain actions that do not belong in any other groups.

If no actions are provided, default actions apply as per **SecDefaultAction (phase:2,log,auditlog,pass)**. The full list of actions are available here:

https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#Actions

When constructing the rules, you can specify at what phase the rule should run. Specifying the correct phase can be beneficial in order to reduce CPU processing.

Rule Syntax

Rule Syntax

Rule Syntax

The following rule looks at the request Uniform Resource Identifier (URI) and tries to match the regular expression pattern <script> against it. The double quotes are used because the second parameter contains a space:

```
SecRule REQUEST_URI "@rx <script>"
```

To split a long line into two, use a single backslash character, followed by a new line:

```
SecRule ARGS KEYWORD \

phase:1,t:none,block
```

Multiple variables can be used in a rule as long as they are separated using the pipe character, for example:

```
SecRule REQUEST_URI|REQUEST_PROTOCOL <script>
```

The **SecDefaultAction** directive is used if no actions are defined for a rule. For example, the following rule:

```
SecRule ARGS D1
```

Is equivalent to:

```
SecRule ARGS D1 phase2:log:auditlog,pass
```

Related Links

- Rule Example 1 – Cross Site Scripting (XSS) Attack
- Rule Example 2 – Whitelist IP Address
- Rule Example 3 – Chaining Rules
- Rule Example 4 – Shellshock Bash Attack

Rule Example 1 – Cross Site Scripting (XSS) Attack

Rule Example 1 – Cross Site Scripting (XSS) Attack

The following rule is used to avoid XSS attacks by checking for a <script> pattern in the request parameters and header and generates an 'XSS Attack' message with a 404 status response.

```
SecRule ARGS|REQUEST_HEADERS "@rx <script>" id:101,msg: 'XSS
```

```
Attack',severity:ERROR,deny,status:404
```

Variables

Details about the variables in this rule example are in the table below:

Variable	Definition
ARGS	Request parameters
REQUEST_HEADERS	All of the request headers

Operator

"@rx <script>" – Performs a regular expression match of the pattern (in this case <script>) provided as a parameter.

Actions

Details of the actions contained in this rule example are provided in the table below:

Action(s)	Description
id, msg, severity, deny, status	These are all of the actions to be performed if the pattern is matched.
id:101	The unique ID that is assigned to the rule (or chain) in which it appears.
msg: "XSS Attack"	The custom message (i.e. XSS Attack) assigned to the rule (or chain) in which it appears.
Severity:ERROR	The severity of the rule. Severities include: • EMERGENCY (0)

Action(s)	Description
	• ALERT (1) • CRITICAL (2) • ERROR (3) • WARNING (4) • NOTICE (5) • INFO (6) • DEBUG (7)
`deny`	This stops rule processing and intercepts transaction. This is a disruptive action.
`status:404`	This specifies the response status code (404) with actions deny and redirect.

Rule Example 2 – Whitelist IP Address

The following example shows how to whitelist an IP address to bypass the ModSecurity engine:

```
SecRule REMOTE_ADDR “@ipMatch 192.168.1.101” \

id:102,phase:1,t:none,nolog,pass,ctl:ruleEngine=off
```

Variables

Variable Name: REMOTE_ADDR

Variable Definition: The IP address of the remote client

Note: Rules listing IP addresses with the /32 subnet mask are not supported and will not upload successfully.

Operator

“@ipMatch 192.168.1.101” – Performs an IPv4 or IPv6 match of the REMOTE_ADDR variable data. In this care – this is the whitelisted IP address.

Actions

Action(s)	Description
`id:101`	The unique ID that is assigned to the rule (or chain) in which it appears.
`phase:1`	Places the rule (or chain) in Phase 1 processing. There are five phases, including: • Request Headers (1) • Request Body (2) • Response Headers (3) • Response Body (4) • Logging (5)
`t:none`	Indicates that no action is used to transform the value of the variable used in the rule before matching. For example, **t:utf8toUnicode** converts all UTF-8 character sequences to Unicode to assist in input normalization.
`nolog`	Prevents rule matches from appearing in both the error and audit logs.
`pass`	Continues processing with the next rule in spite of a successful match.
`ctl:ruleEngine=off`	This action changes ModSecurity configuration on a transient, per-transaction basis. This only affects the transaction in which the action is executed. In this case, the ModSecurity rule engine is turned off.

Rule Example 3 – Chaining Rules

Rule Example 3 – Chaining Rules

Chained rules allow for more complex rule matches where a number of different VARIABLES are used to create a better rule and to help prevent false positives. In programming language concepts – think of chained

rules as somewhat similar to AND conditional statements. The actions specified in the first portion of the chained rule will only be triggered if all of the variable checks return positive hits. If one aspect of the chained rule is negative, then the entire rule chain is negative. The most unique portion should be specified on the first line – this will reduce the number of “normal” requests that will have to be evaluated against the rest of the chained rule set.

In addition to using a number of different VARIABLES in the one rule, it is also possible to chain more than one rule. Below is an example of chaining two rules. In this example, the first rule checks if the username (**ARGS:username**) for the string admin (**streq admin**) using a string comparison. If the first rule holds true, the second rule is activated which denies all requests that are not from the REMOTE_ADDR 192.168.1.111 IP Address (**!streq 192.168.1.111**).

```
SecRule ARGS:username “@streq admin” chain,deny

SecRule REMOTE_ADDR “!streq 192.168.1.111”
```

Rule Example 4 – Shellshock Bash Attack

Rule Example 4 – Shellshock Bash Attack

This section shows an example of the rules requires to mitigate the Shellshock Bash attack. There are two rules needed in this case. Details of both rules are provided in the sections below.

First Rule

This is the first rule:

```
SecRule REQUEST_LINE|REQUEST_HEADERS|REQUEST_HEADERS_NAMES "@contains () {"
"phase:1,id:'2100080',block,t:none,t:utf8toUnicode,t:urlDecodeUni,t:compressWhi
tespace,msg:'SLR: Bash ENV Variable Injection
Attack',tag:'CVE-2014-6271',tag:'http://cve.mitre.org/cgi-bin/
cvename.cgi?name=CVE-2014-6271',tag:'https://securityblog.redhat.com/2014/09/
24/bash-specially-crafted-environment-variables-code-injection-attack/'"
```

Variables

Details about the variables in this example rule are provided in the table below:

Variable	Definition
REQUEST_LINE	This variable holds the complete request line sent to the server (including the request method and HTTP version information).

Variable	Definition
`REQUEST_HEADERS`	All of the request headers
`REQUEST_HEADERS_NAMES`	All of the names of the request headers.

Operator

`"@contains () {" - Checks the REQUEST_LINE|REQUEST_HEADERS|REQUEST_HEADERS_NAMES variables for the string '() {' and returns true if found.`

Actions

Action(s)	Description
`phase:1`	Places the rule (or chain) in Phase 1 processing. There are five phases, including: • Request Headers (1) • Request Body (2) • Response Headers (3) • Response Body (4) • Logging (5)
`id:'2100080'`	The unique ID that is assigned to this rule (or chain) in which it appears.
`block`	This performs the disruptive action defined by the previous SecDefaultAction. This allows rule writers to request a blocking action without specifying how the blocking is to be done. The **SecRuleUpdateActionById** directive allows you to override how a rule handles blocking. Please refer to the Rule Block Function section for further details.

Action(s)	Description
`t:none`	Indicates that no action is used to transform the value of the variable used in the rule before matching.
`t:utf8toUnicode`	Converts all UTF-8 character sequences to Unicode to assist in input normalization.
`t:urlDecodeUni`	Decodes a URL-encoded input string with support for the Microsoft-specific %u encoding.
`t:compressWhitespace`	Converts any of the whitespace characters (0x20, \f, \t, \n, \r, \v, 0xa0) to spaces (ASCII 0x20), compressing multiple consecutive space characters into one.
`msg:'SLR: Bash ENV Variable Injection Attack',tag:'CVE-2014-6271'`	The custom message (i.e. XSS Attack) assigned to the rule (or chain) in which it appears.

`tag:'http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271'`
 	
`tag:'https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/'`
	Assigns a tag (category) to a rule (or chain). This is metadata allows easy automated categorization of events. Multiple tags can be specified on the same rule.

Second Rule

The second rule is as follows:

```
SecRule REQUEST_BODY "@contains () {"
"phase:2,id:'2100081',block,t:none,t:utf8toUnicode,t:urlDecodeUni,t:compressWhi
tespace,msg:'SLR: Bash ENV Variable Injection
Attack',tag:'CVE-2014-6271',tag:'http://cve.mitre.org/cgi-bin/
cvename.cgi?name=CVE-2014-6271',tag:'https://securityblog.redhat.com/2014/09/
24/bash-specially-crafted-environment-variables-code-injection-attack/'"
```

Variables

Variable Name: REQUEST_BODY

Variable Definition: All of the request body.

Operator

"@contains () {" – Checks the **REQUEST_BODY** variable for the string **'() {'** and returns true if found.

Actions

Action(s)	Description
`phase:2`	Places the rule (or chain) in Phase 2 processing. There are five phases, including: • Request Headers (1) • Request Body (2) • Response Headers (3) • Response Body (4) • Logging (5)
`id:'2100081'`	The unique ID that is assigned to this rule (or chain) in which it appears.
`block`	This performs the disruptive action defined by the previous SecDefaultAction. This allows rule writers to request a blocking action, but without specifying how the blocking is to be done. The **SecRuleUpdateActionById** directive allows you to override how a rule handles blocking. Please refer to the Rule Block Function section for further details.
`t:none`	Indicates that no action is used to transform the value of the variable used in the rule before matching.
`t:utf8toUnicode`	Converts all UTF-8 character sequences to Unicode to assist in input normalization.
`t:urlDecodeUni`	Decodes a URL-encoded input string with support for the Microsoft-specific %u encoding.

Action(s)	Description
`t:compressWhitespace`	Converts any of the whitespace characters (0x20, \f, \t, \n, \r, \v, 0xa0) to spaces (ASCII 0x20), compressing multiple consecutive space characters into one.
`msg:'SLR: Bash ENV Variable Injection Attack',tag:'CVE-2014-6271'`	The custom message (i.e. XSS Attack) assigned to the rule (or chain) in which it appears.

`tag:'http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271'`
 	
`tag:'https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/'`
	Assigns a tag (category) to a rule (or chain). This is metadata which allows easy automated categorization of events. Multiple tags can be specified on the same rule.

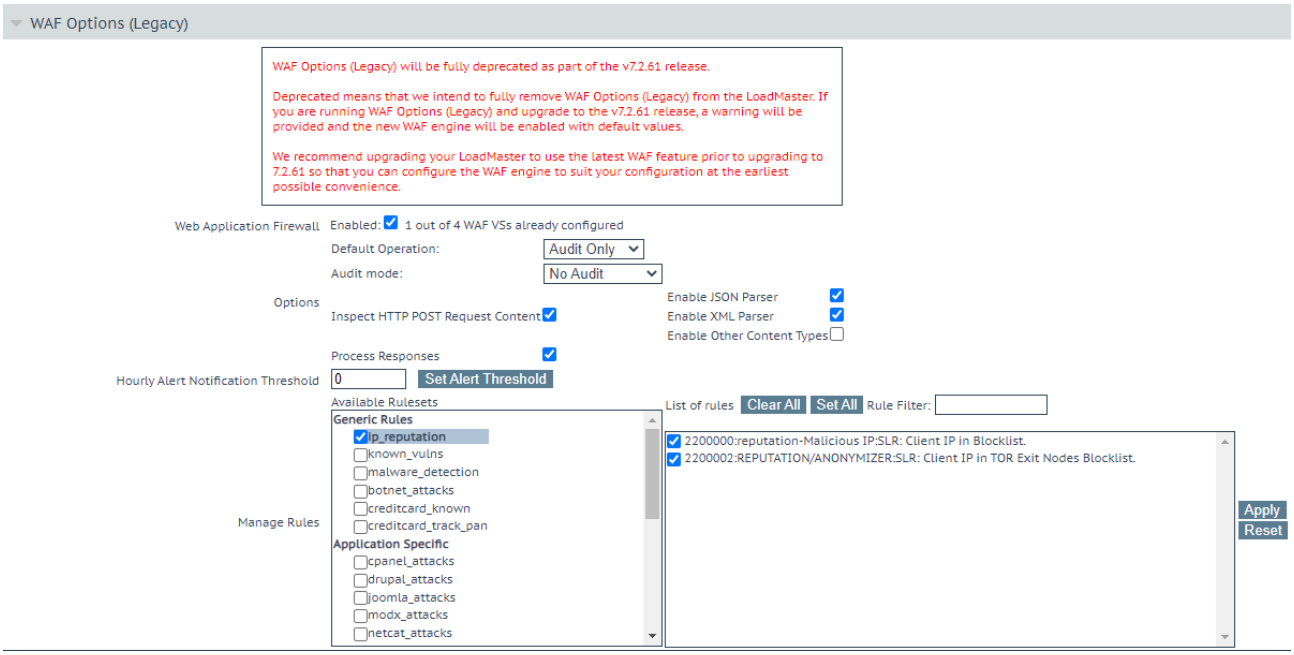
WUI Settings

WUI Settings

In the LoadMaster Web User Interface (WUI), WAF settings can be configured for each individual Virtual Service.

Note: The Legacy WAF functionality is not available on new LoadMaster deployments of firmware version 7.2.59 or above. If you have upgraded from a pre-7.2.59 version to 7.2.59 the Legacy WAF functionality remains available.

CAUTION: The legacy WAF Options (**WAF Options (Legacy)**) will be fully deprecated as part of the v7.2.61 release.Deprecated means that Progress Kemp intend to fully remove **WAF Options (Legacy)** from the LoadMaster. If you are running **WAF Options (Legacy)** and upgrade to the v7.2.61 release, a warning will be provided and the new WAF engine will be enabled with default values.We recommend upgrading your LoadMaster to use the latest WAF feature prior to upgrading to 7.2.61 so that you can configure the WAF engine to suit your configuration at the earliest possible convenience.



In the **WAF Options** section of the Virtual Service modify screen (**Virtual Services > View/Modify Services > Modify**), there is a drop-down list called **Default Operation**. The **Default Operation** can be set to **Audit Only** or **Block Mode**.

The **Audit Only** mode of operation sets the **SecDefaultAction** to **phase:2,log,auditlog,pass**.

The **Block Mode** of operation sets the **SecDefaultAction** to **phase:2,log,auditlog,block,drop**.

Rule Block Function

Rule Block Function

The rule block function is quite complicated. This section offers further explanation of the rule block function. The following example has been taken from https://github.com/Spiderlabs/ModSecurity/wiki/Reference-Manual#block and further explanatory text has been added.

```
The block action is essentially a placeholder that is intended to be used by
rule writes to request a blocking action, but without specifying how the
blocking is to be done. The SecDefaultAction command specifies how the blocking
is to be done. The block action is a placeholder that will be replaced by the
action from the last SecDefaultAction in the same context.
```

Block Example 1

The following example shows the **SecDefaultAction** set to **deny**. The second rule will “deny” because the **SecDefaultAction** is set to **deny**.

```
SecDefaultAction phase:2,deny,id:101,status:403,log,auditlog
```

```
SecRule ARGS attack2 phase:2,pass,id:103

SecRule ARGS attack1 phase:2,block,id:102
```

Block Example 2

The following example shows the usage of the **SecRuleUpdateActionById** command to override how a rule handles blocking. The **SecRuleUpdateActionById** command allows a rule to be reverted back to the previous **SecDefaultAction**. In this example, the first rule (**SecRule ARGS attack1 phase:2,deny,id:1**) would deny based on meeting the successful conditions associated with the rule.

By using the **SecRuleUpdateActionById** against rule **Id 1** and indicating block, we are associating the first rule action to that of the **SecDefaultAction** which is pass. So in the case, the first rule would pass based on meeting the successful conditions associated with the rule; it would not deny.

```
SecDefaultAction phase:2,pass,log,auditlog

SecRule ARGS attack1 phase:2,deny,id:1

SecRuleUpdateActionById 1 block
```

3

Managing Custom WAF Rules in the LoadMaster

Managing Custom WAF Rules in the LoadMaster

Refer to the following sections for details on managing custom WAF rules in the LoadMaster.

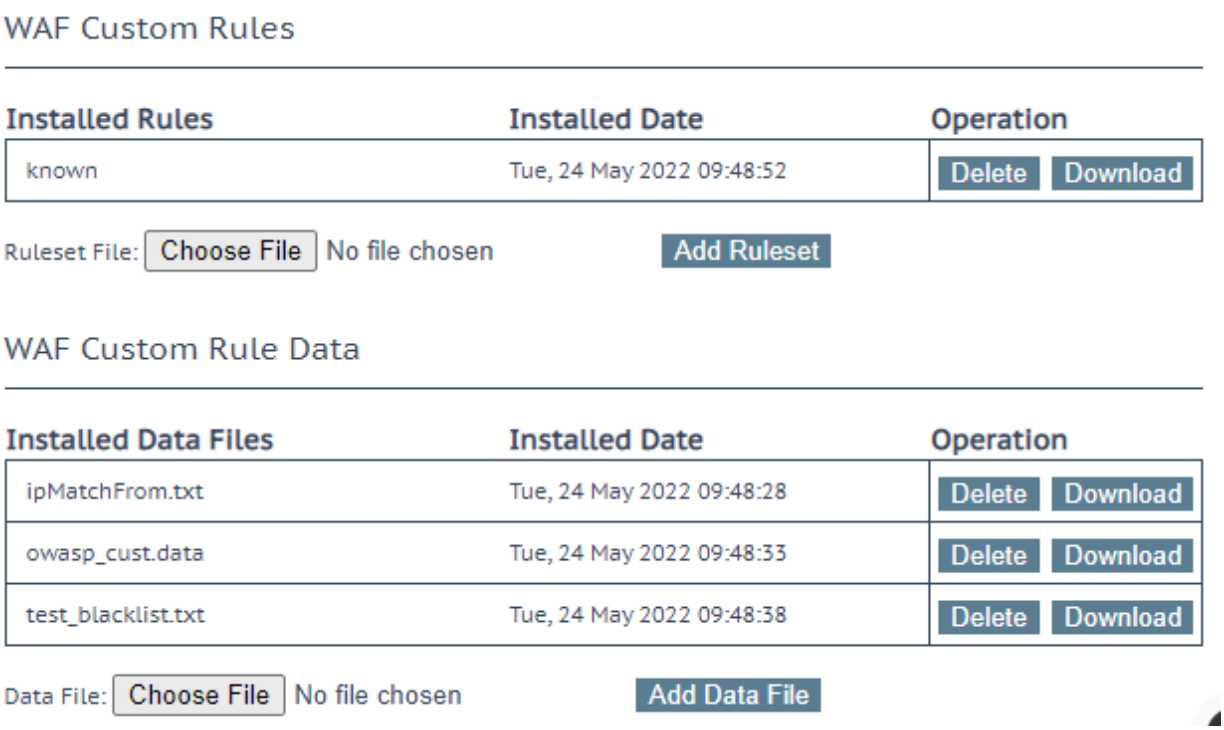
Related Links

- Add a Custom Rule
- Delete/Download a Custom Rule or Data File

Add a Custom Rule

Follow the steps below to find out how to add custom WAF rules in the Web User Interface (WUI) of the LoadMaster:

1. In the main menu, select **Web Application Firewall > Custom Rules**.



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

   Note: Individual rules can be uploaded as .conf files, or you can load a package of rules in a tar.gz file. The first character in the filename must be an alpha character or an underscore (_). The other characters in the filename can include full stops (.) or dashes (-).

   Note: Rules listing IP addresses with the /32 subnet mask are not supported and will not upload successfully.

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

   Note: The additional files are for the rules' associated data files. If using a Tarball, the rules and data files can be packaged together.

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

The rules will now be available to assign within the Virtual Services modify screen (**Virtual Services > View/ Modify Services > Modify**). Refer to the Assigning Custom Rules to a Virtual Service section to find out how to configure the Virtual Service.

Delete/Download a Custom Rule or Data File

Delete/Download a Custom Rule or Data File



Custom rules and data files can be deleted or downloaded by clicking the relevant buttons.

Note: If a rule is assigned to a Virtual Service, it will not be available for deletion.

4

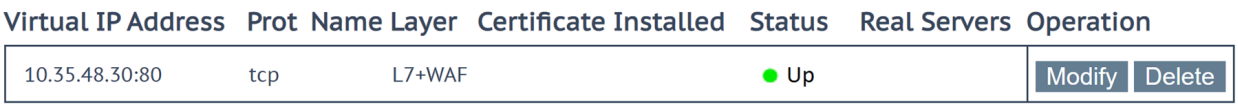
Assigning Custom Rules to a Virtual Service

Assigning Custom Rules to a Virtual Service

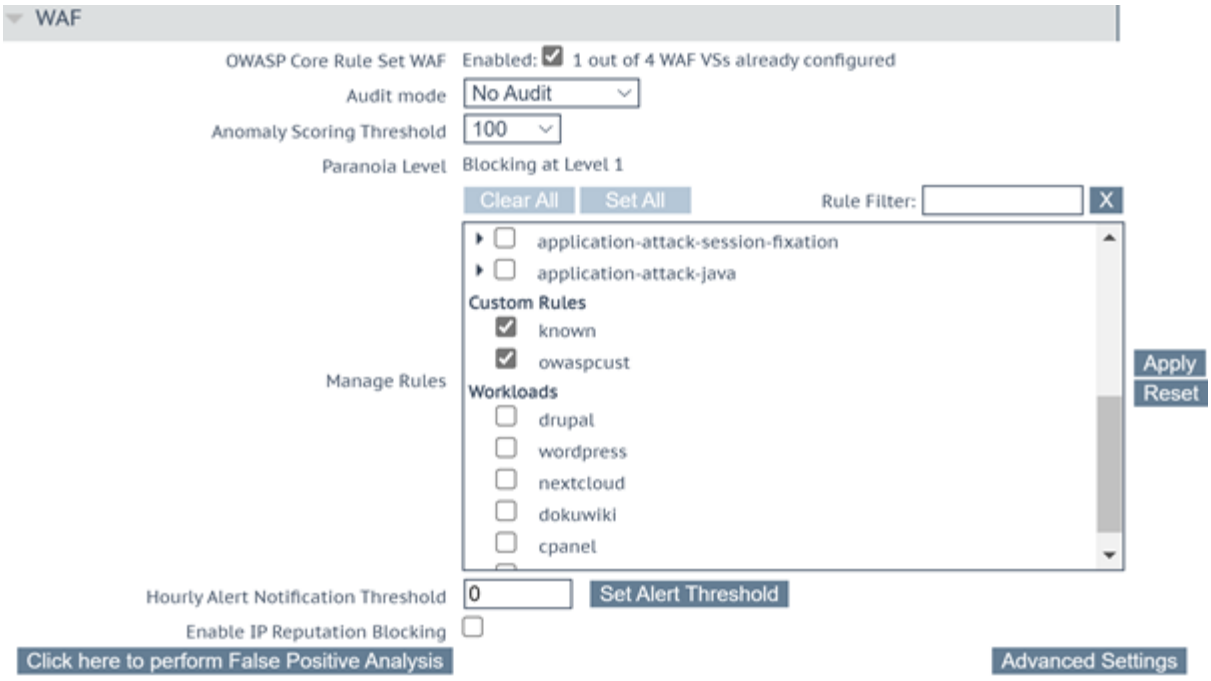
Before you can assign a custom rule to a Virtual Service, the rule must first be installed on the LoadMaster. Refer to the Add a Custom Rule section for instructions on how to do this.

Custom rules can be assigned as needed to each individual Virtual Service. Follow the steps below to assign a custom rule to a Virtual Service:

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** section.



4. Select **Enabled**.

Note: A message is displayed next to the **Enabled** check box displaying how many WAF-enabled Virtual Services exist and it also displays the maximum number of WAF-enabled Virtual Services that can exist. If the maximum number of WAF-enabled Virtual Services has been reached, the **Enabled** check box becomes greyed out.

---

5. Assign Custom Rules by selecting them in the **Manage Rules** section.
6. To enable/disable the individual rules per ruleset, select/unselect the relevant check boxes.Rules can be filtered by entering a filter term in the **Rule Filter** text box.When you have a filter entered, you can do the following:
   - Click **Clear All** to disable all rules for the selected ruleset.
   - Click **Set All** to enable all rules for the selected ruleset.
   - Click **Reset** to disable all rules and rulesets.

Note: There is a **Run First** check box available for custom rules. If the **Run First** check box is enabled for a custom rule, the rule will be run first, before the OWASP Core Rule Set (CRS). If the **Run First** check box is disabled for a custom rule, the custom rule runs after the CRS. The **Run First** check box is disabled by default.

---

7. When finished selecting the relevant rulesets and rules, click **Apply**.

Related Links

- WAF Misconfigured State

WAF Misconfigured State

WAF Misconfigured State

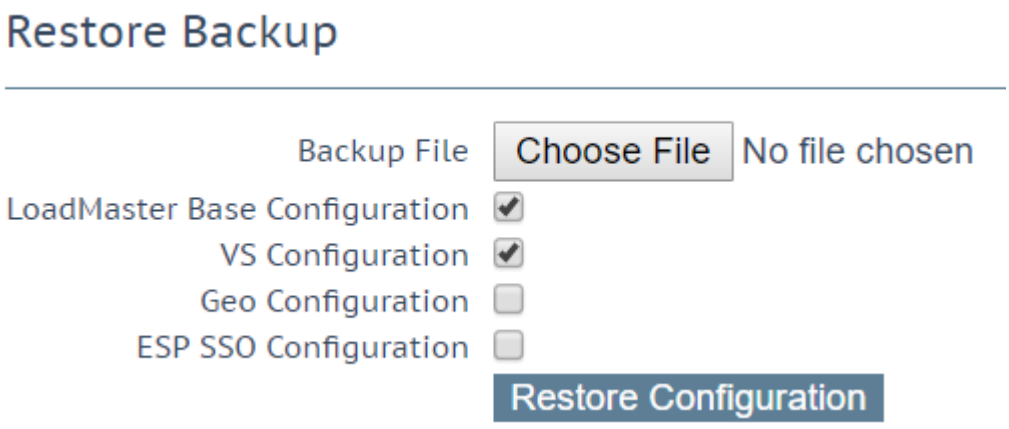


On the **View/Modify Services** screen in the LoadMaster WUI, the **Status** of each Virtual Service is displayed. If the WAF for a particular Virtual Service is misconfigured, for example if there is an issue with a rule file, the status changes to **WAF Misconfigured** and turns to red. If the Virtual Service is in this state, all traffic is blocked. WAF can be disabled for that Virtual Service to stop the traffic being blocked, if required, while troubleshooting the problem.

5

Backing Up and Restoring WAF Configuration

Backing Up and Restoring WAF Configuration



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**.

Note: A WAF configuration can only be restored onto a LoadMaster with an WAF license.

6

References

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

ModSecurity Reference Manual https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual

Web Application Firewall, Feature Description

LoadMaster, Product Overview