

# FortiADC Web Application Firewall (WAF) Basic Deployment Guide

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



Friday, January 25 2019

FortiADC WAF Basic Deployment Guide

First Edition

---

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>Configuration overview</b> .....	<b>6</b>
<b>Configurations</b> .....	<b>7</b>
To configure a WAF Profile.....	7
To configure a Web Attack Signature policy.....	8
To configure a URL Protection policy.....	9
To configure an HTTP Protocol Constraint policy.....	10
To configure an SQL/XSS Injection Detection policy.....	11
To configure an exception object.....	12
To configure a Bot Detection policy.....	13
To configure XML Detection.....	14
To configure JSON Detection.....	15
To import an XML schema file.....	16
To import an XML schema file.....	17
Configuring a HTTP Virtual Server and referring WAF Profile.....	18
<b>Monitor</b> .....	<b>20</b>

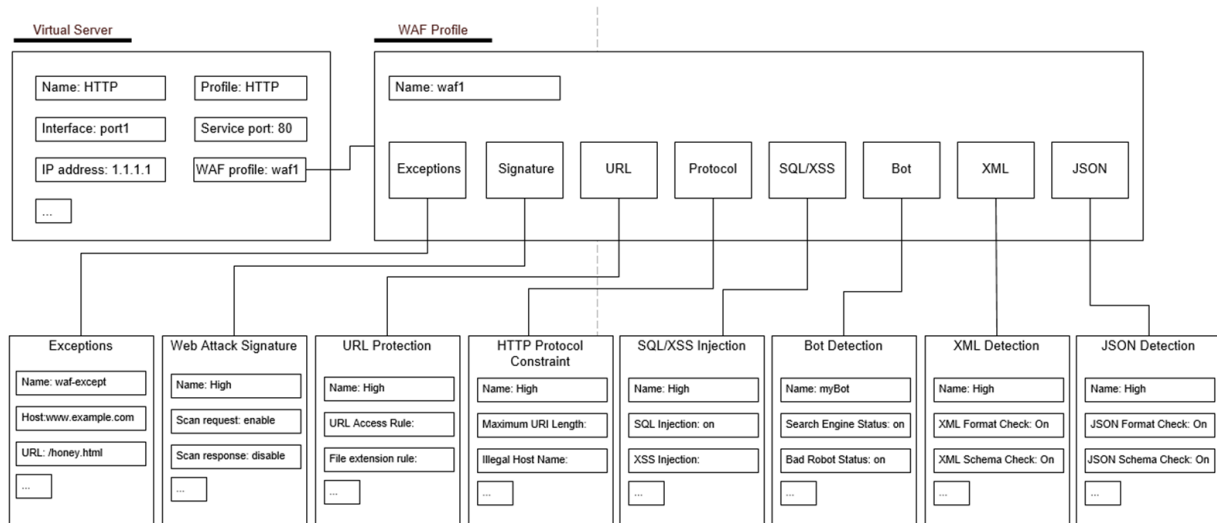
# Change Log

Date	Change Description
1/25/2019	First release.

# Introduction

A Web Application Firewall (WAF) is a security policy that protects hosted web applications from known and unknown attacks and filter matching traffics. This document includes the basic configuration of WAF feature on FortiADC.

# Configuration overview



# Configurations

## Configuring a WAF Profile

We provide three predefined WAF profiles as following shown:

Please refer to [table 76](#) from FortiADC handbook 5.1.0

If desired, you can create user-defined profiles based on the following steps.

## To configure a WAF Profile

1. Go to Web Application Firewall.
2. Click the **WAF Profile** tab.
3. Click **Create New** to display the configuration editor.
4. Fill in the **Name** as “waf1”.
5. Fill in the **Web Attack Signature** as “High-Level-Security”.
6. Fill in the **HTTP Protocol Constraint** as “High-Level-Security”.
7. Fill the **SQL/XSS Injection Detection** as “High-Level-Security”.
8. Click **Save** to save the configuration.

The screenshot shows a configuration window titled "WAF Profile" with a close button (X) in the top right corner. The window contains several input fields and dropdown menus:

- Name:** A text input field containing "waf1".
- Description:** A text input field with the placeholder text "Optional description."
- Web Attack Signature:** A dropdown menu with "High-Level-Security" selected.
- URL Protection:** A dropdown menu with "Click to select" as the current selection.
- HTTP Protocol Constraint:** A dropdown menu with "High-Level-Security" selected.
- SQL/XSS Injection Detection:** A dropdown menu with "High-Level-Security" selected.
- Exception Name:** A dropdown menu with "Click to select" as the current selection.
- Bot Detection Name:** A dropdown menu (partially visible at the bottom).

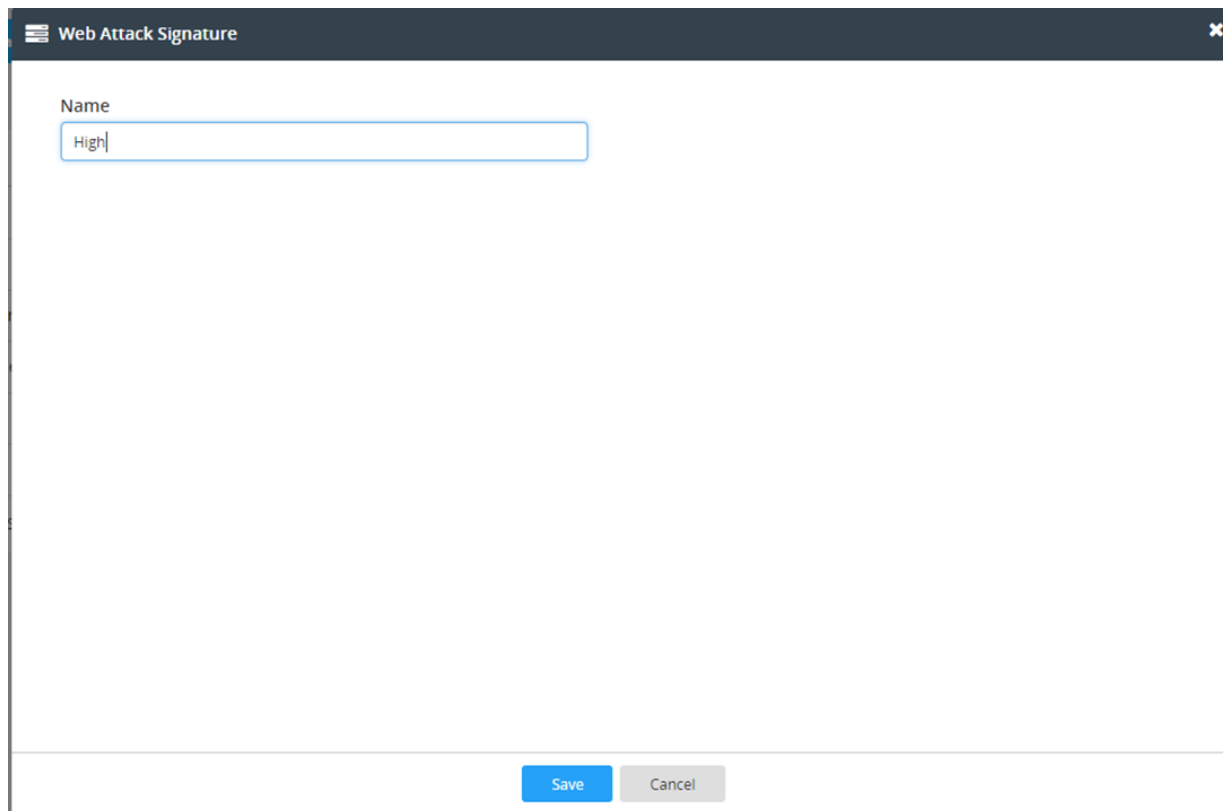
At the bottom of the window, there are two buttons: a blue "Save" button and a grey "Cancel" button.

Now, we have a WAF profile named “waf1” using three basic features with predefined modes.

In addition, you can create more WAF related user-defined policies based on the following steps.

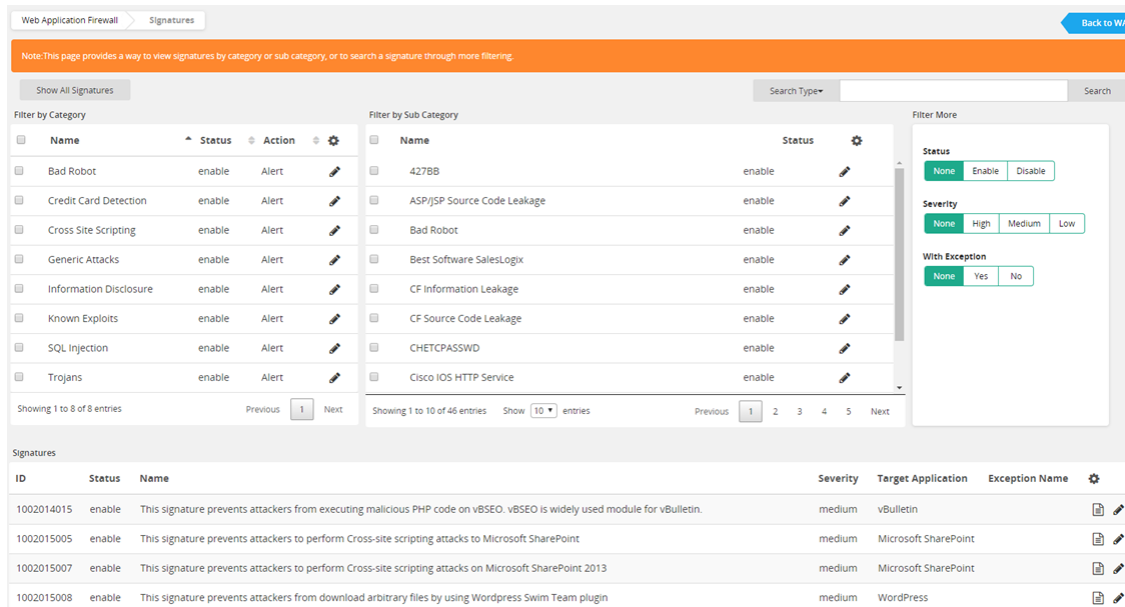
## To configure a Web Attack Signature policy

1. Go to Web Application Firewall.
2. Click the **Web Attack Signature** tab.
3. Click **Create New** to display the configuration editor.
4. Fill in the **Name** as “High”.
5. Click **Save** to save the configuration.



The screenshot shows a configuration window titled "Web Attack Signature". Inside the window, there is a label "Name" above a text input field containing the text "High". At the bottom of the window, there are two buttons: "Save" (highlighted in blue) and "Cancel" (greyed out).

6. Click the **View** to display the view signature page.



7. Choose the **Signature** based on the **Category** and **Sub Category** from the configuration editor page showing above. You can use the right top window to filter the signature based on Status, Severity or With Exception. (For the detailed information, please refer to the [FortiADC Handbook > Chapter 8: Web application firewall overview.](#))

## To configure a URL Protection policy

1. Go to **Web Application Firewall**.
2. Click the **URL Protection** tab.
3. Click **Create New** to display the configuration editor.
4. Fill in the **Name** as “High”.
5. Click **Save** to save the configuration.
6. Click **Edit** to display the configuration editor.
7. Click **Create New** in URL Access Rule part to display the configuration editor and fill the Full URL Pattern, Action, and Severity based on your security requirements.
8. Click **Create New** in File Extension Rule part to display the configuration editor and fill the File Extension Pattern, Action, and Severity based on your security requirements.

URL Protection
✕

Name

**URL Access Rule**

▼ Add Filter Create New

<input type="checkbox"/>	ID	Full URL Pattern	Action	Severity	
<input type="checkbox"/>	1	https://10.106.168.1/ui/?vdom=vdom1_with_long_name_sib_ftp_test_lalalalalalalalala_hawaii#/navigate/Config/waf/waf	Alert	Low	✎ ✕ 📄

Showing 1 to 1 of 1 entries    Show  entries    Previous  Next

**File Extension Rule**

▼ Add Filter Create New

<input type="checkbox"/>	ID	File Extension Pattern	Action	Severity	
<input type="checkbox"/>	1	/Config/waf/waf	Alert	Medium	✎ ✕ 📄

Showing 1 to 1 of 1 entries    Show  entries    Previous  Next

Save
Cancel

## To configure an HTTP Protocol Constraint policy

1. Go to **Web Application Firewall**.
2. Click the **HTTP Protocol Constraint** tab.
3. Click **Create New** to display the configuration editor.
4. Fill in the **Name** as "High".
5. Modify all options based on your requirements.
6. **Save** the configuration.

	Length	Action	Severity
Name	High		
Maximum URI Length	2048	Alert	Low
Illegal Host Name	OFF	Alert	Low
Illegal Http Version	OFF	Alert	Low
Illegal Http Multipart	OFF	Alert	Low
Maximum Cookie Number In Request	16	Alert	Low
Maximum Header Number In Request	50	Alert	Low
Maximum Request Header Name Length	1024	Alert	Low
Maximum Request Header Value Length	4096	Alert	Low
Maximum URL Parameter Name Length	1024	Alert	Low
Maximum URL Parameter Value Length	4096	Alert	Low
Maximum Request Header Length	8192	Alert	Low

## To configure an SQL/XSS Injection Detection policy

1. Go to **Web Application Firewall**.
2. Click the **SQL/XSS Injection Detection** tab.
3. Click **Create New** to display the configuration editor.
4. Fill in the **Name** as "High".
5. **Enable** SQL Injection Detection and XSS Injection Detection.
6. Modify those options under SQL Injection Detection and XSS Injection Detection based on your requirements.
7. **Save** the configuration.

**SQL/XSS Injection Detection**

Name  
High

SQL Injection Detection  
 ON

SQL Injection Detection

URI Detection  
 OFF

Cookie Detection  
 OFF

Action  
 Alert  Deny

XSS Injection Detection  
 ON

XSS Injection Detection

URI Detection

Referer Detection  
 OFF

Body Detection  
 OFF

Severity  
 High  Medium  Low

Referer Detection

Save Cancel

## To configure an exception object

1. Go to **Web Application Firewall**.
2. Click the **Exceptions** tab.
3. Click **Create New** to display the configuration editor.
4. Fill in the **Name** as "waf-exception".
5. **Save** the configuration.
6. Click the **Edit** to display the configuration editor.
7. Click **Create New** to display the Exception Rule configuration editor.
8. **Enable** Exception Host Status.
9. Fill in the Host Pattern as ftp://mozilla.org/.
10. Fill in the URL Pattern as "/Config/waf/waf"
11. **Save** the configuration

Exceptions ✕

[Edit Exception Rule](#)

Exception Host Status

ON

Host Pattern

URL Pattern

Maximum length is 127 characters

[Save](#) [Cancel](#)

## To configure a Bot Detection policy

1. Go to **Web Application Firewall**.
2. Click the **Bot Detection** tab.
3. Click **Create New** to display the configuration editor.
4. Fill in the **Name** as "High".
5. Enable the **Status**.
6. Enable the Search Engine Status.
7. Enable Bad Robot Status.
8. Modify the HTTP Request Rate, Action, or Severity based on your requirements.
9. **Save** the configuration.

**Bot Detection**

Name  
High

Status  
 ON

Search Engine Status  
 ON

Bad Robot Status  
 ON

HTTP Request Rate  
0  
Default: 0 Range: 0-100000000

Action  
 Alert  Deny  Period Block

Severity  
 High  Medium  Low

WhiteList

Save Cancel

## To configure XML Detection

1. Go to Web Application Firewall > XML & JSON Validation and select the XML Detection tab.
2. Click **Create New**.
3. Fill in the **Name** as "High".
4. Modify all the options based on your requirements. (For the details of all options, please [refer](#) to the FortiADC Handbook > Chapter 8: Web Application Firewall > Configuring XML Detection.)
4. Click **Save**.

The screenshot shows a configuration window titled "XML Detection". It features a "Name" input field containing the text "High". Below this are six toggle switches for various checks: "XML Format Check" (ON), "Soap Format Check" (OFF), "XML Schema Check" (OFF), "XML Limit Check" (OFF), "XML XSS Check" (OFF), and "XML SQL Injection Check" (OFF). At the bottom of the window, there is a "Severity" label and two buttons: "Save" and "Cancel".

## To configure JSON Detection

1. Go to Web Application Firewall > XML & JSON Validation and select the JSON Detection tab.
2. Click **Create New**.
3. Fill in the **Name** as "High".
4. Enable JSON Format Check.
5. Modify all the options based on your requirements.
6. Click **Save**.

**JSON Detection**

Name  
High

JSON Format Check  
ON

JSON Schema Check  
ON

JSON Schema

JSON Limit Check  
ON

Max Array Value  
256

**Notes:**

For the XML schema and JSON schema, please import the files before referring.

**To import an XML schema file**

1. Go to Web Application Firewall > XML & JSON Validation and select the **XML Schema** tab.
2. Click Create New.
3. Enter the **name** of the XML schema configuration. You will use the name to select the schema file in XML detection profiles. No spaces.
4. Click Choose File and select the XML schema file that you want to import.
5. Click **Save**.

XML Schema ✕

Name

File

Choose File unique.zip ✕

Please select a file to upload.

---

Save Cancel

### To import an XML schema file

1. Go to Web Application Firewall > XML & JSON Validation and select the **JSON Schema tab**.
2. Click **Create New**.
3. Enter the **Name** as "json\_schema1". You will use the name to select the schema file in JSON detection profiles. No spaces.
4. Click **Choose File** and select the JSON schema file that you want to import.
5. Click **Save**.

JSON Schema ✕

Name  
schema1

File  
Choose File jsonschema\_all.zip ✕  
Please select a file to upload.

Save Cancel

## Configuring a HTTP Virtual Server and referring WAF Profile

To Configure a L7 SLB Virtual Server:

1. Go to Server Load Balance > Virtual Server
2. Click **Create New**.
3. Fill the **Name** as "HTTP\_VS1".
4. Choose the **Application** as "HTTP(S)".
5. Enter the IP address, Port and Interface based on your requirements.
6. Create a Real Server Pool and refer it in Real Server Pool.
7. Click **Save**.

**Basic Edit**

**Name**  
Required config name. No spaces.

**Application**  
HTTP(S)

**Address**  
1.1.1.1  
Example: 192.0.2.1 2001:0db8::1

**Port**  
80  
Range: 0 or 1-65535.

**Interface**  
port5

**Real Server Pool**  
HTTP1

**SSL**  
 Enable

**Save** **Cancel**

8. Click **Edit** to display the configuration editor page.
9. Go to the **Security** page.
10. Choose the WAF Profile “waf1” we just created above in the WAF Profile.
11. Click **Save**.

# Monitor

You can use the FortiADC logs to verify that packet flow is working as expected.

Before reviewing the security logs, please enable the security log under **Log & Report > Security Category > WAF**.

**Local Log**

ON

**Event Category**

Configuration  Admin  System  User  Health Check

SLB  LLB  GLB  Firewall  Enable All

Required. Please select at least one category.

**Traffic**

ON

Traffic logging should be used mainly for debugging; traffic logging will consume extensive memory and CPU resources. Please disable traffic logging after debugging is complete.

**Traffic Category**

SLB  GLB  LLB  Enable All

Required. Please select at least one category.

**Security**

ON

**Security Category**

Synflood  IP Reputation  WAF  GEO  AV  Enable All

Required. Please select at least one category.

**Script**

OFF

**Save** **Cancel**

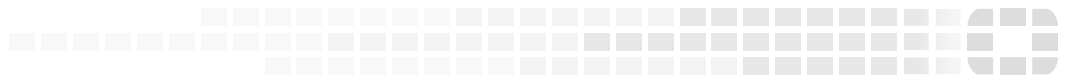
To check the security logs for Layer 7 HTTP virtual servers, go to **Log & Report > Log Browsing > Security Log > WAF**.

Date	Time	Severity	Source	Destination	Action
2018-06-25	11:58:12	medium	192.213.13.220	192.213.13.60	pass
2018-06-25	11:45:44	medium	192.213.13.220	192.213.13.60	pass
2018-06-25	11:45:29	medium	192.213.13.220	192.213.13.60	pass
2018-06-25	11:44:53	medium	192.213.13.220	192.213.13.60	pass
2018-06-25	11:44:41	medium	192.213.13.220	192.213.13.60	pass

<span>Event Log</span> <b><span>Security Log</span></b> <span>Traffic Log</span> <span>Script Log</span> <span>Aggregate Log</span>						
<input type="radio"/> IP Reputation <input type="radio"/> SYNflood <input checked="" type="radio"/> WAF <input type="radio"/> GEO						
<span>Filter Setting</span> <span>Download</span> <span>Refresh</span>						
Date	Time	Severity	Source	Destination	Action	
2018-06-25	11:58:12	medium	192.213.13.220	192.213.13.60	pass	
<b>Date</b>	2018-06-25	<b>Time</b>	11:58:12	<b>Log Level</b>	alert	
<b>Log ID</b>	0202006005	<b>Severity</b>	medium	<b>VS Name</b>	7000	
<b>Message ID</b>	32740201	<b>Source</b>	192.213.13.220	<b>Source Port</b>	40378	
<b>Service</b>	http	<b>Destination</b>	192.213.13.60	<b>Destination Port</b>	7000	
<b>Source Country</b>	United States	<b>Destination Country</b>	United States	<b>Sub Type</b>	waf	
<b>Type</b>	attack	<b>Action</b>	pass	<b>Http Host</b>	192.213.13.60:7000	
<b>Vdom</b>	root	<b>Packet Header</b>	POST / HTTP/1.1 Host: 192.213.13.60:7000 User-Agent: curl/7.46.0 Accept: */* Content-Length: 1209233 Expect: 100-continue			
<b>Http URL</b>	/	<b>User Agent</b>	curl/7.46.0			
<b>Message</b>	"Attack ID: 1010030014 NAME: "Illegal HTTP Multipart/form-data Encoding" CATEGORY: "HTTP Protocol Constraint" SUB_CATEGORY: "HTTP Multipart Check"					
<b>Method</b>	POST					



High Performance Network Security



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.