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

Friday, January 25 2019

FortiADC WAF Basic Deployment Guide

First Edition

TABLE OF CONTENTS

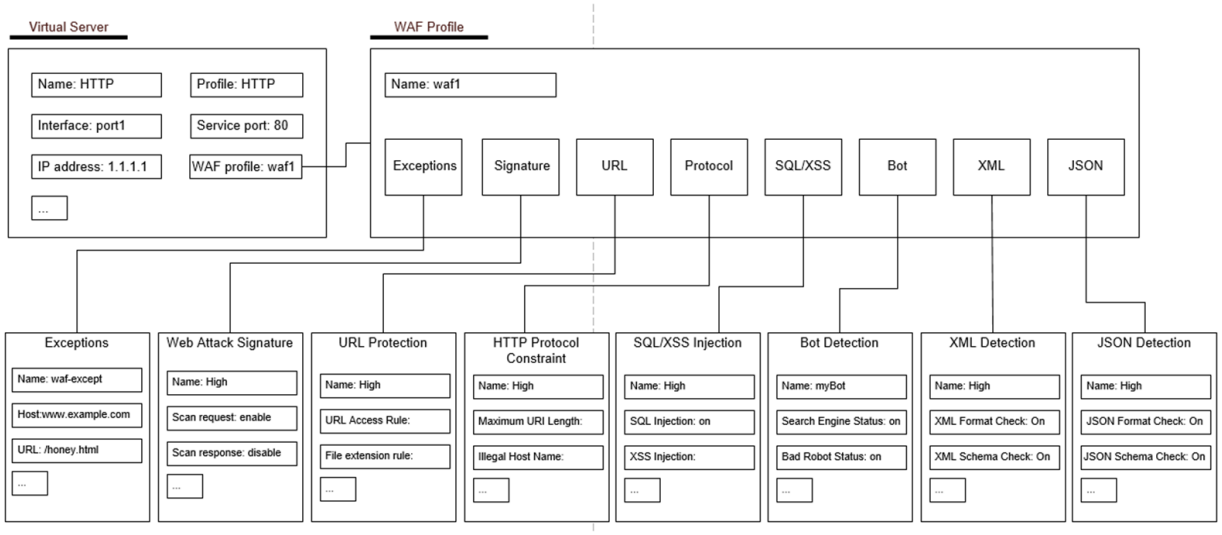
Change Log

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

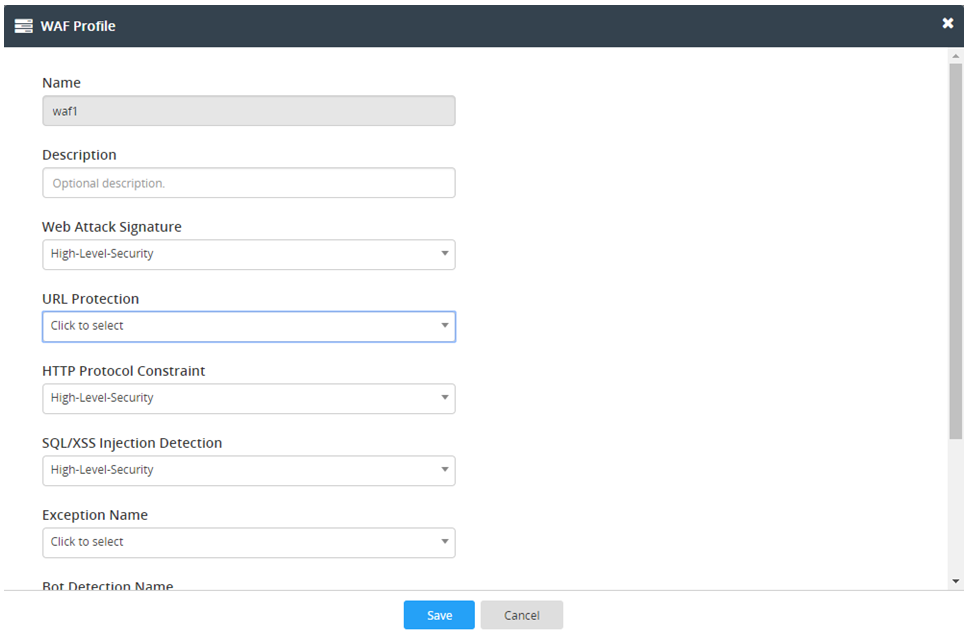
We provide three predefined WAF profiles as following shown:

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.

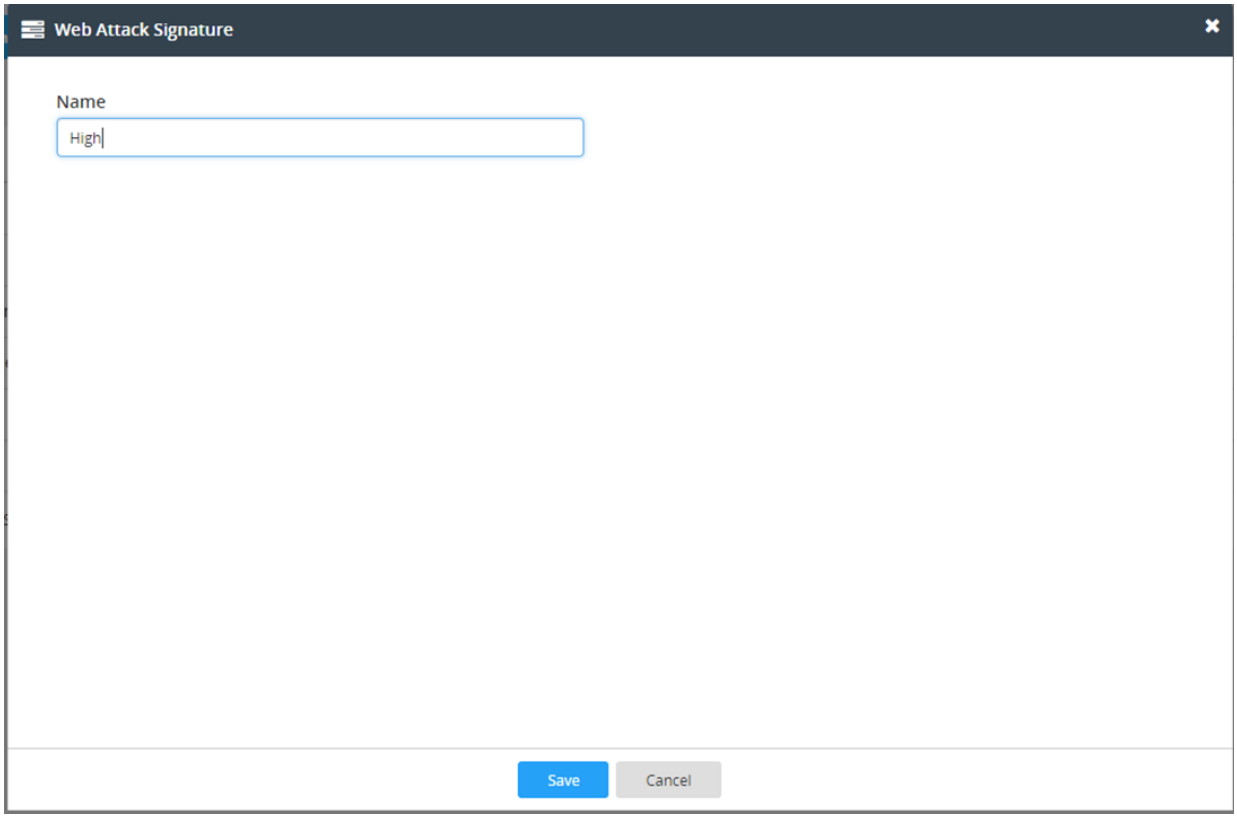


Now, we have a WAF profile named “waf1” using three basic features with predefined modes.

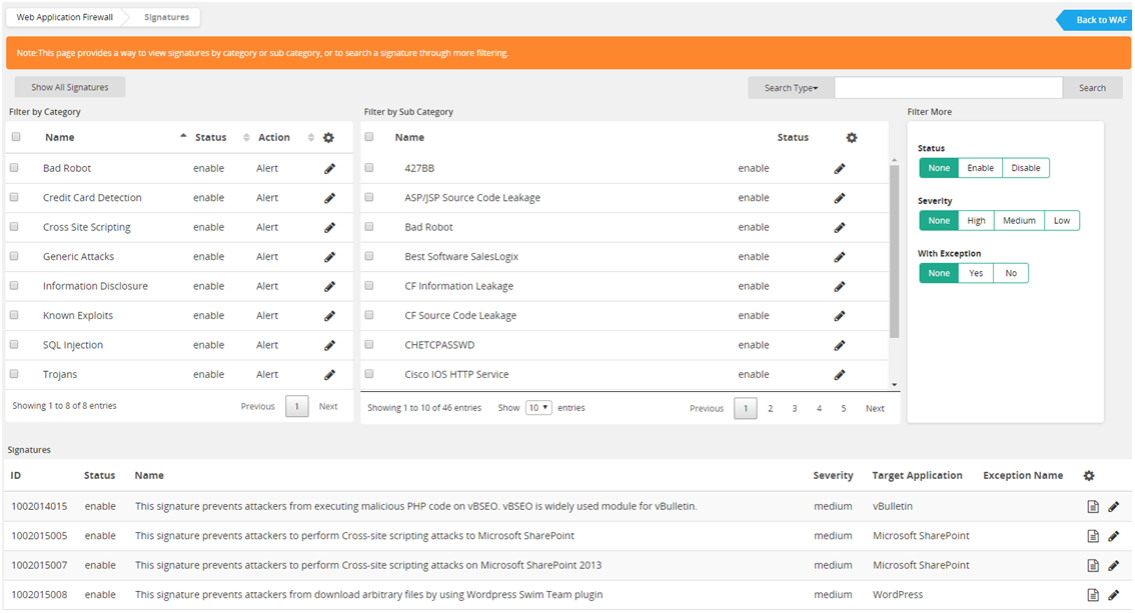
In addition, you can create more WAF related user-defined policies based on the following steps.

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.



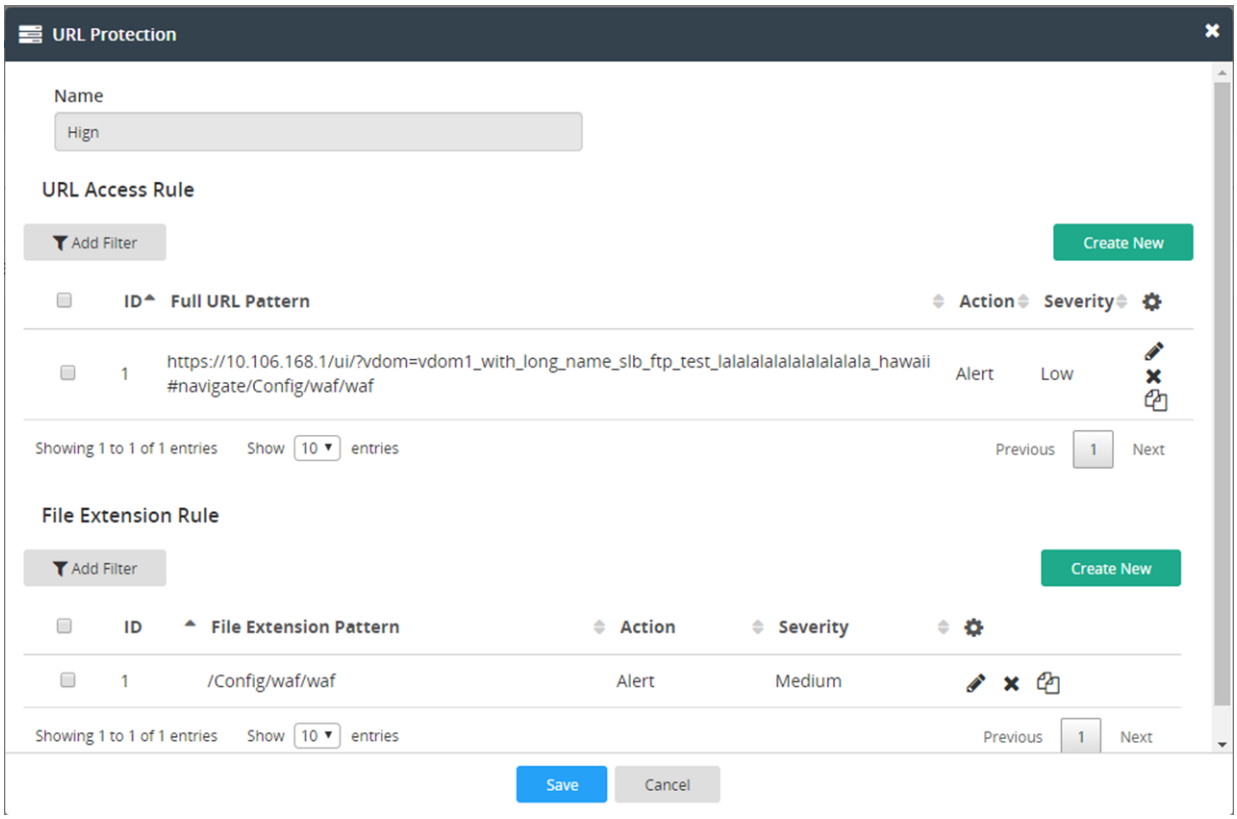
6. Click the **View** to display the view signature page.



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.)

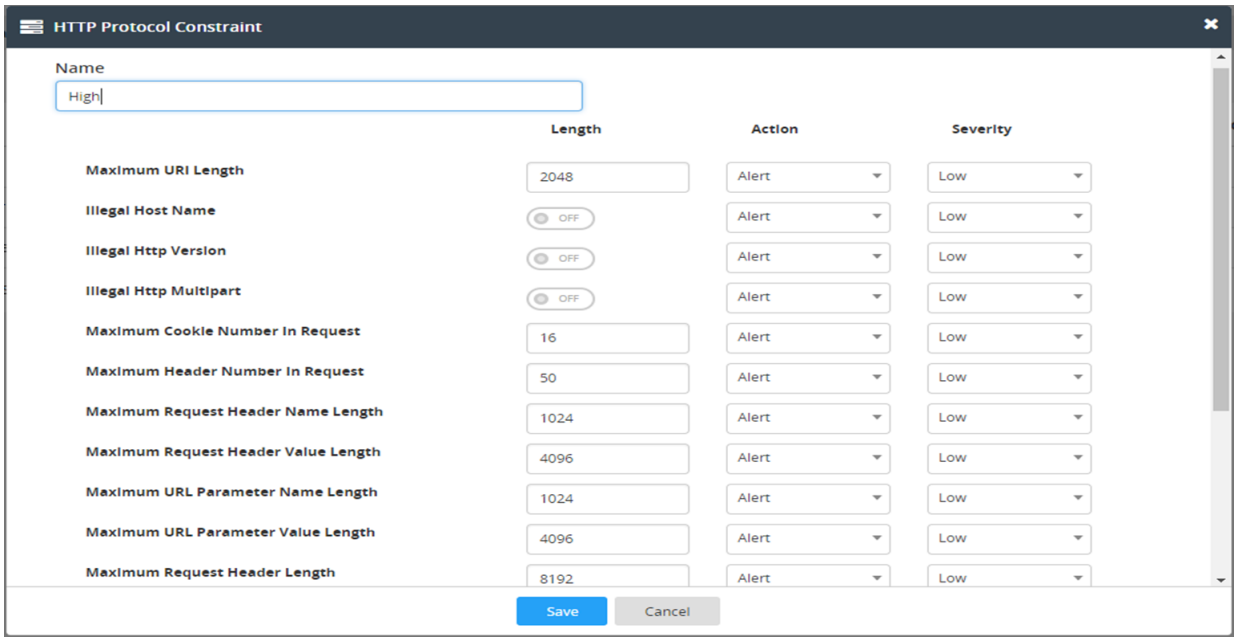
To configure a URL Protection policy

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.



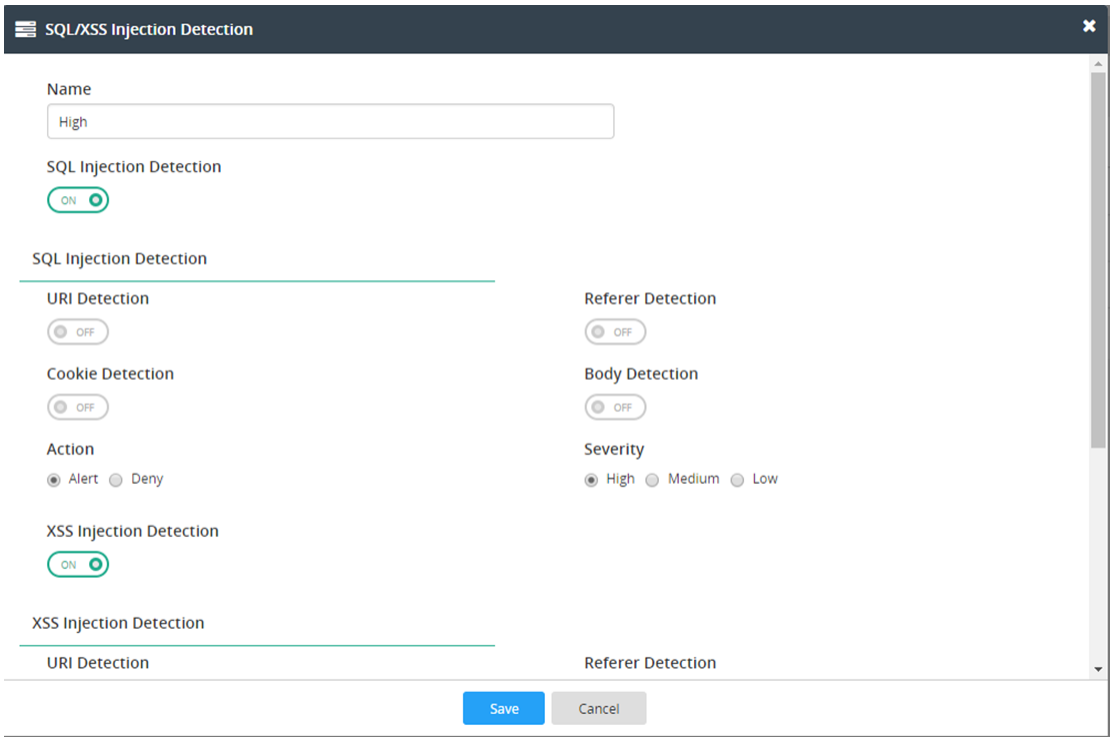
To configure an HTTP Protocol Constraint policy

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.



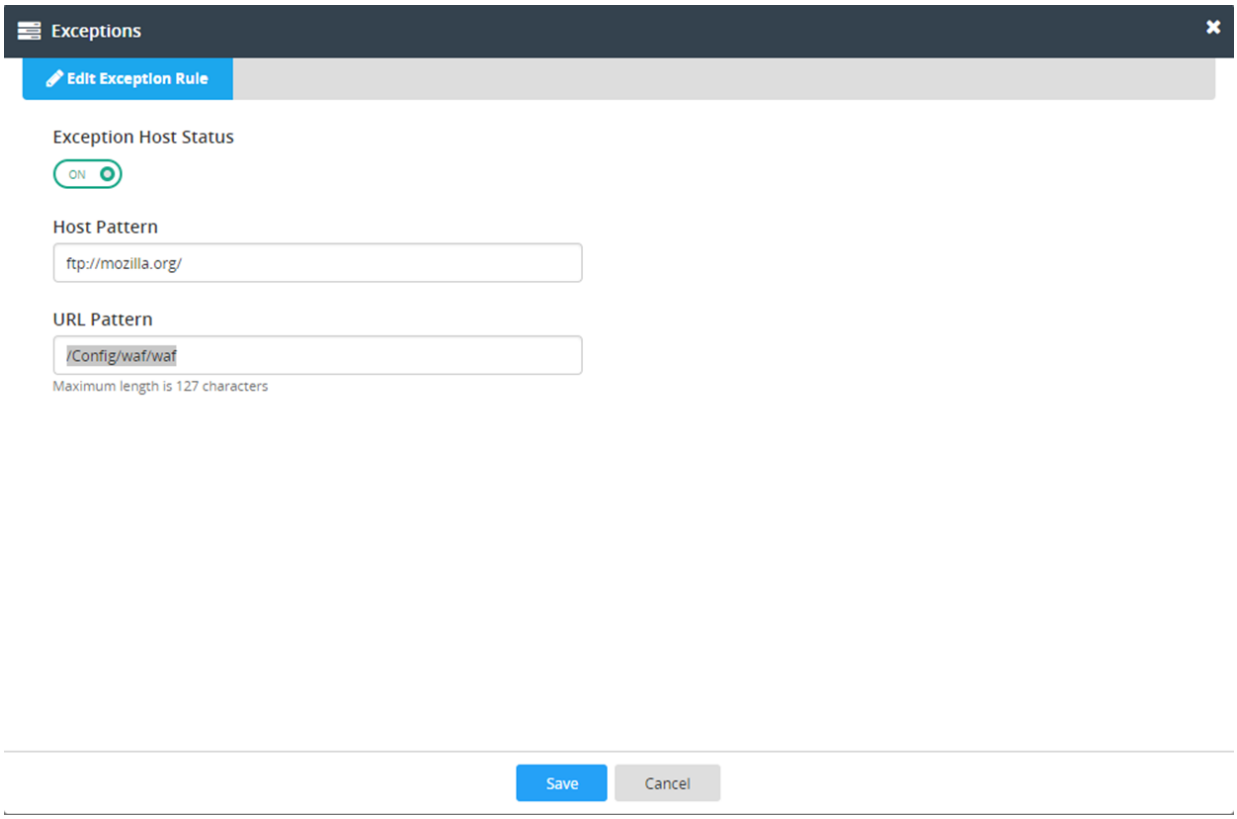
To configure an SQL/XSS Injection Detection policy

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.



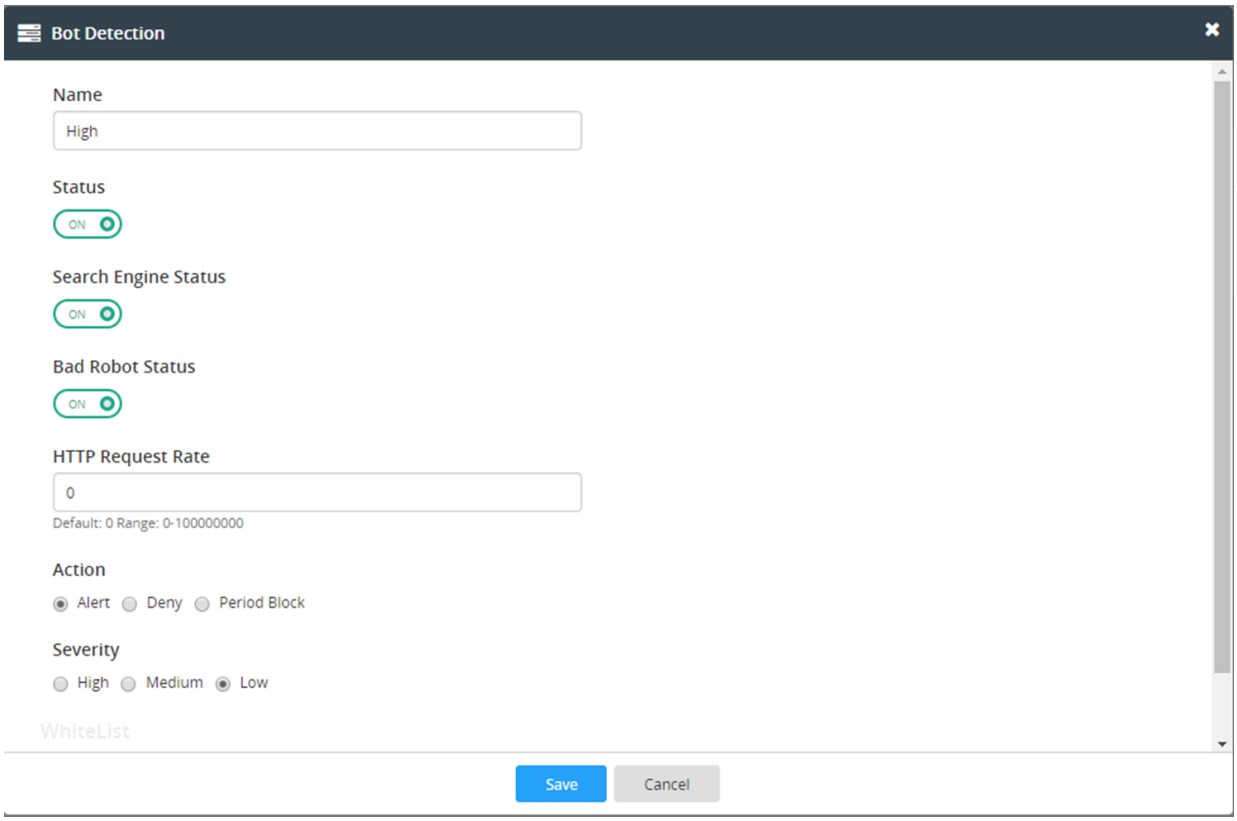
To configure an exception object

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-except”.
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



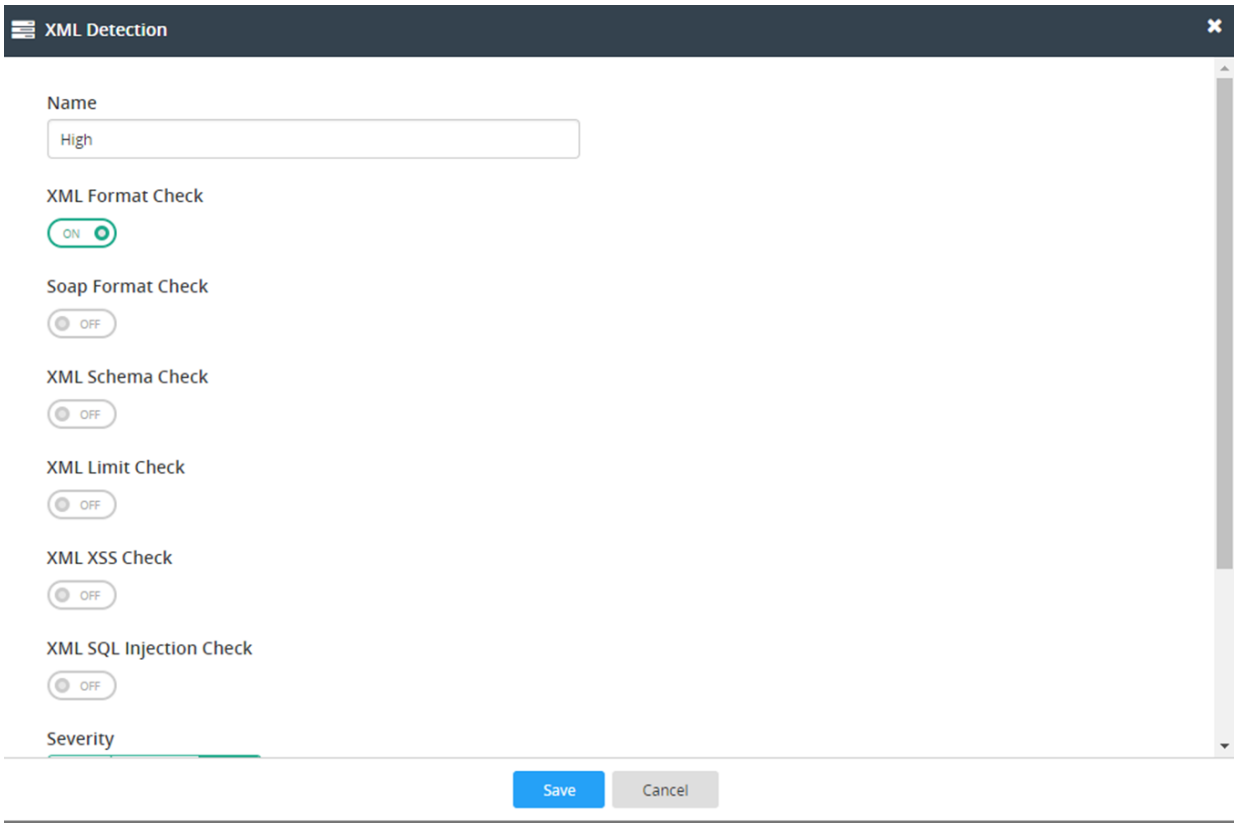
To configure a Bot Detection policy

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.



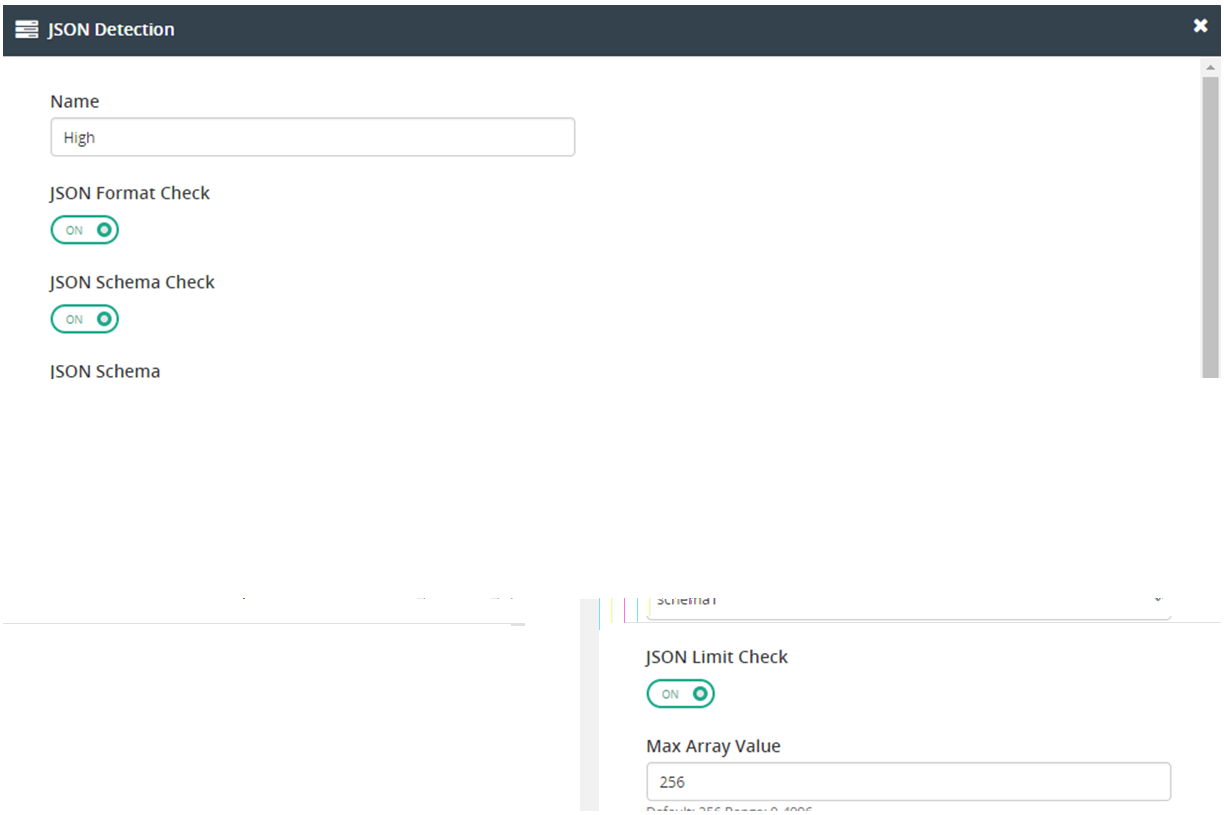
To configure XML Detection

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**.



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**.

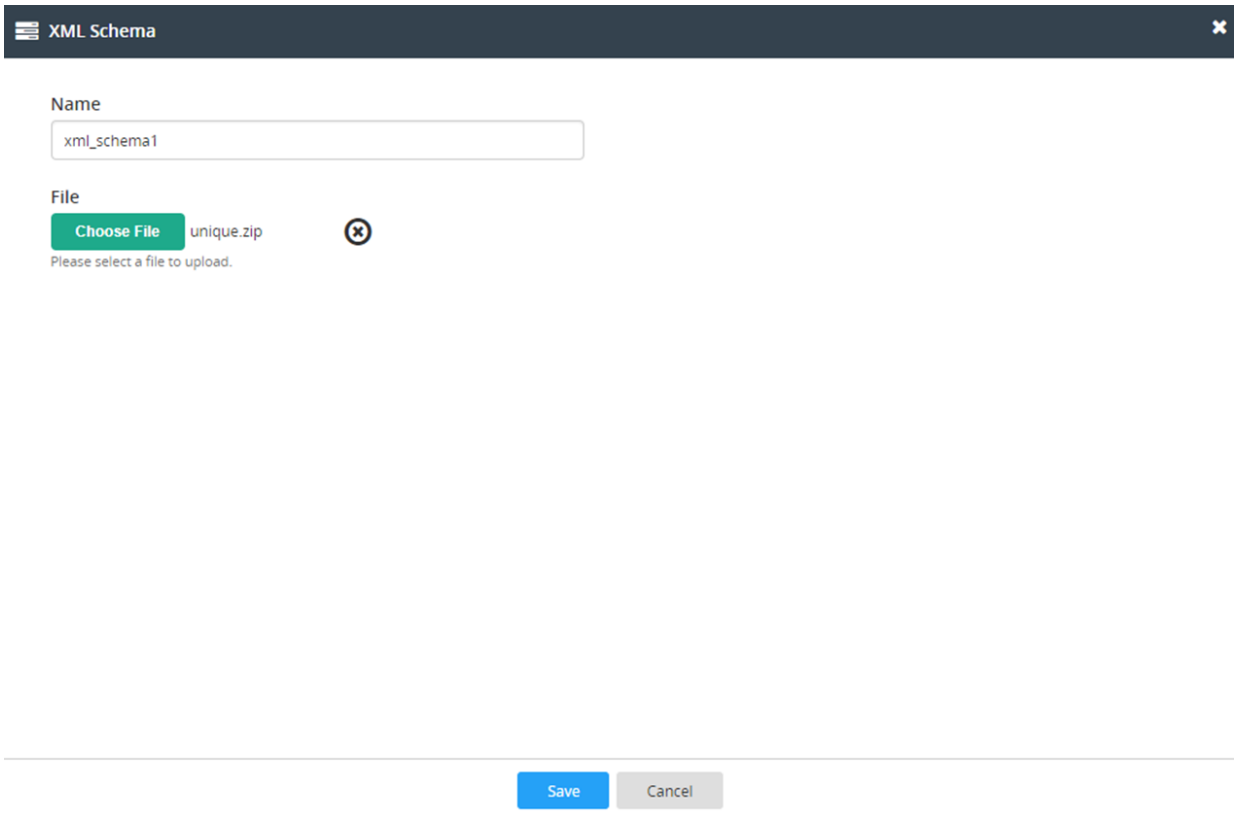


Notes:

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

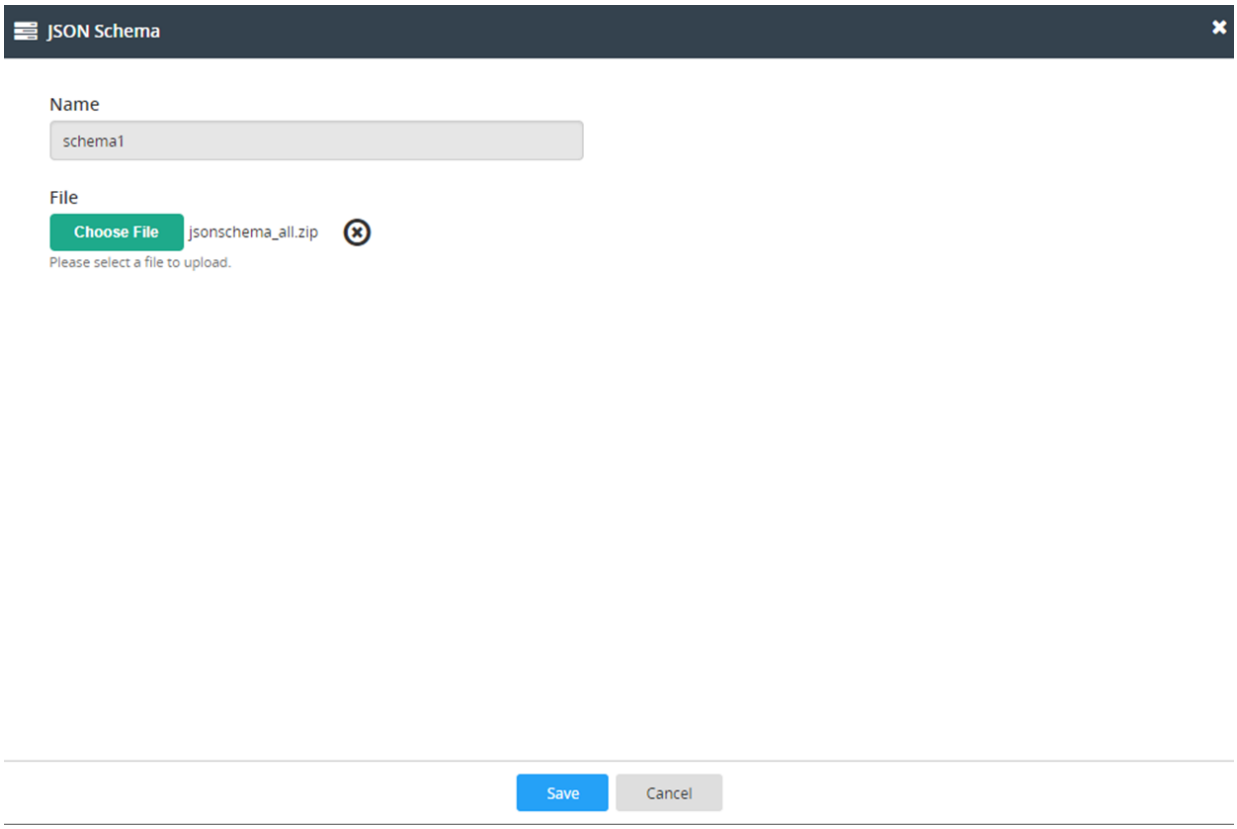
To import an XML schema file

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**.



To import an XML schema file

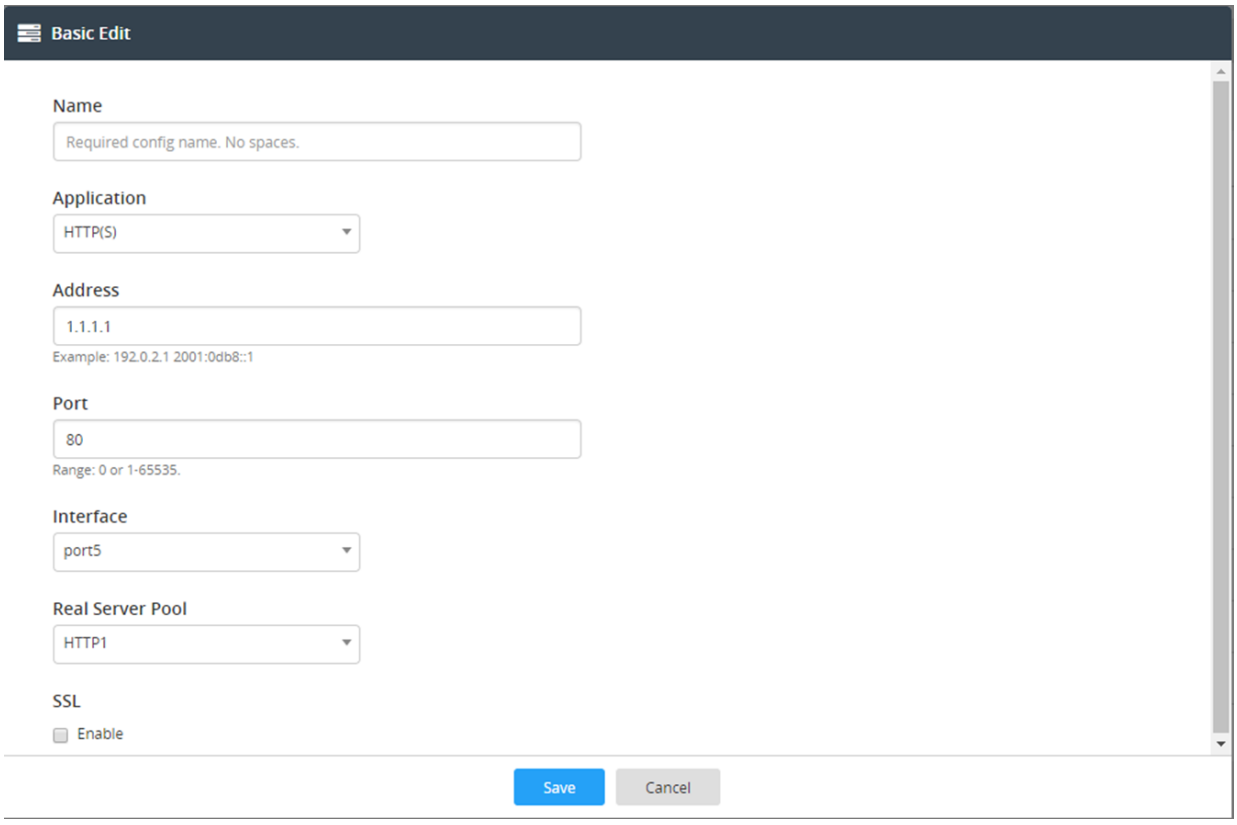
1. Go to Web Application Firewall > XML & JSON Validation and select the **JSON Schema tab**.
2. Click **Create New.**
3. Enter the **Name** as “json_schema1”. You will use the name to select the schema file in JSON detection profiles. No spaces.
4. Click **Choose File** and select the JSON schema file that you want to import.
5. Click **Save**.



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**.

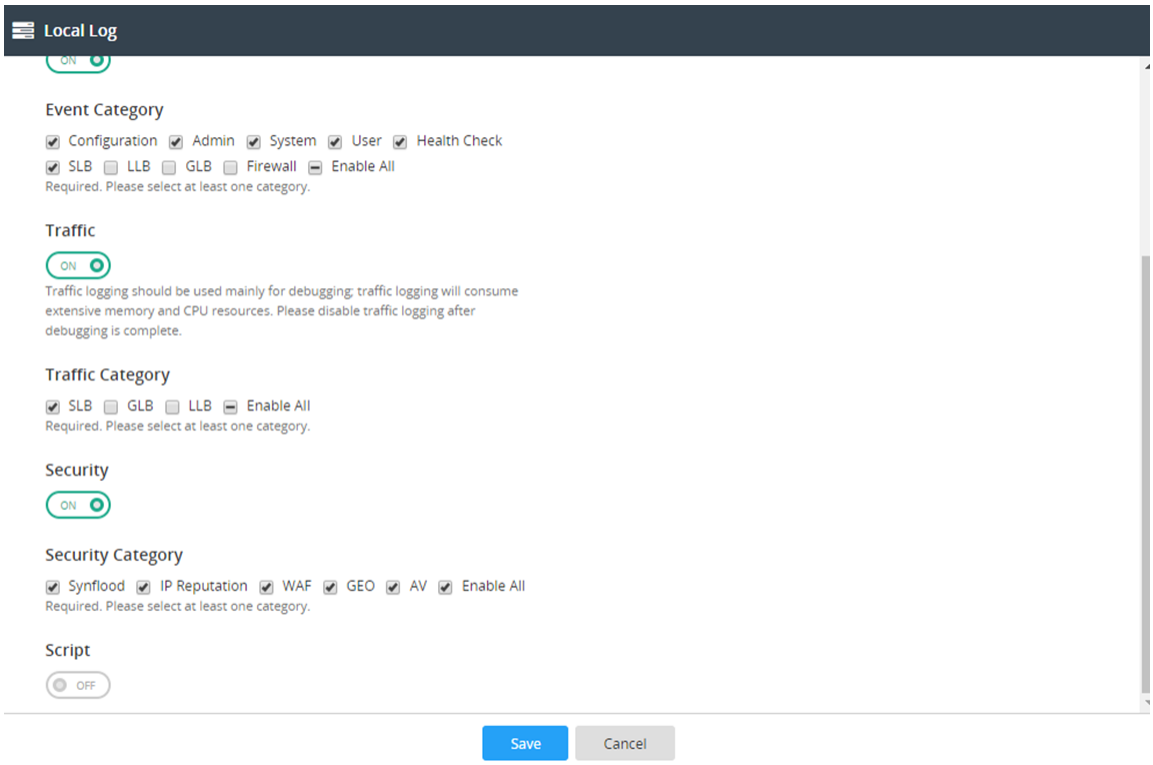


8. Click **Edit** to display the configuration editor page.
9. Go to the **Security** page.
10. Choose the WAF Profile “waf1” we just created above in the WAF Profile.
11. Click **Save**.

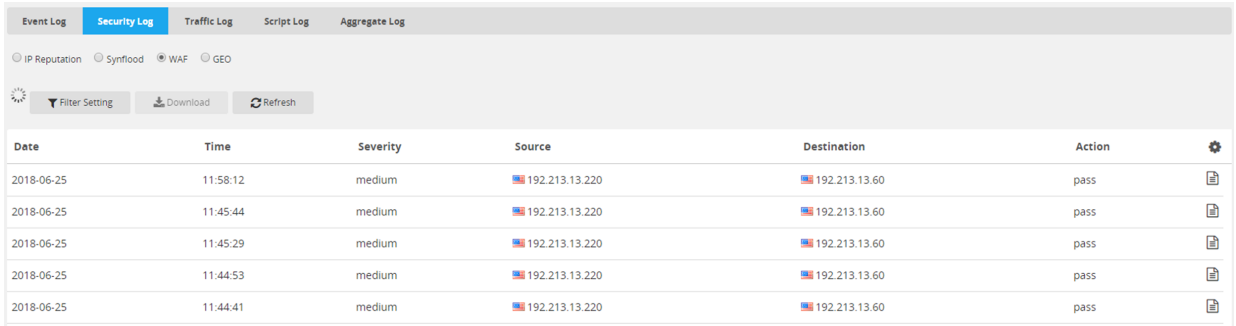
Monitor

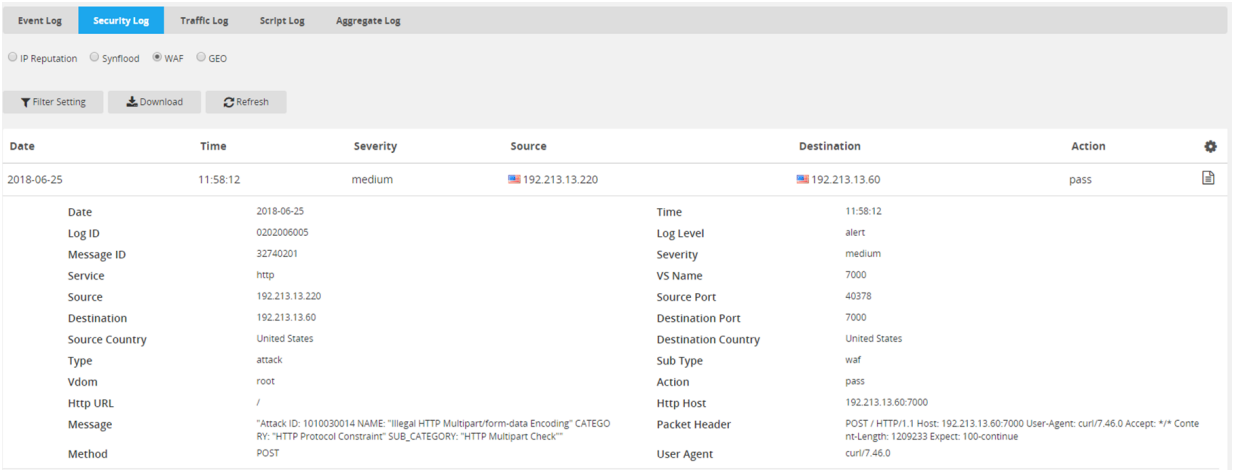
You can use the FortiADC logs to verify that packet flow is working as expected.

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



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




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