



SOFTWARE VERSION
2.0.0

EdgeWAF Free Edition

Administrator User Guide

Document Properties

Document Number: 2.0.10.30.23.10.10

Document Creation Date: 5 August 2021

Document Last Edited: 30 October 2023

Document Author: Jay Savoor

Document Last Edited by:

Document Disclaimer

This manual's screenshots and graphics may differ slightly from your product due to differences in product release. Edgenexus ensures that they make every reasonable effort to ensure that the information in this document is complete and accurate. Edgenexus makes changes and corrections to the information in this document in future releases when the need arises. Edgenexus assumes no liability for any errors.

Copyrights

© 2023. All rights reserved.

Information in this document is subject to change without prior notice and does not represent a commitment on the manufacturer's part. No part of this guide may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of the manufacturer. Registered trademarks are properties of their respective owners. Every effort is made to make this guide as complete and accurate as possible, but no warranty of fitness is implied. The authors and the publisher shall have neither responsibility nor liability to any person or entity for loss or damages arising from using the information contained in this guide.

Trademarks

Edgenexus logo, Edgenexus, EdgeADC, EdgeWAF, EdgeWAF, EdgeDNS are all Edgenexus Limited's trademarks. All other trademarks are the properties of their respective owners and are acknowledged.

Edgenexus Support

If you have any technical questions regarding this product, please raise a support ticket at:
support@edgenexus.io

Table of Contents

Document Properties	1
Document Disclaimer	1
Copyrights.....	1
Trademarks.....	1
Edgenexus Support	1
WAF Explained.....	3
How does the EdgeWAF know what to block or not?	3
Installing the EdgeWAF App.....	4
Getting the EdgeWAF from the App Store.....	4
Downloading and importing the App using the EdgeADC.....	6
Download and import the App using direct download	6
Making the EdgeWAF App operational	6
Using the EdgeWAF	8
The Dashboard	8
The Events Page	9
The Filter Editor	10
Firewall	11
Firewall Control	11
DoS Evasion	12
Management.....	12
Management Navigation Menu	12
Config.....	13
Users.....	13
Info	14
How to use the EdgeWAF	15

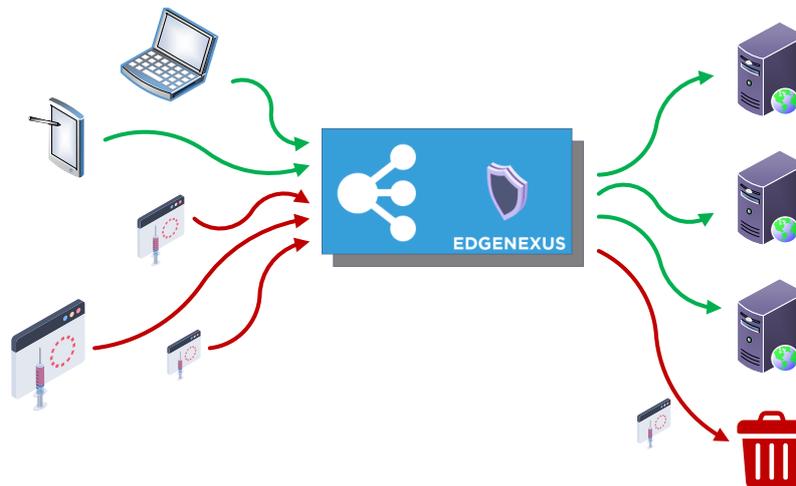
WAF Explained

What is a WAF or Web Application Firewall?

Designed to help protect web-based applications, a WAF works by monitoring all HTTP traffic sent to the web application and filtering out any harmful requests that may be present within the traffic stream. Typically, a WAF protects against attacks such as cross-site forgery and scripting (XSS) and others like SQL injection, file inclusion, and DDoS (Denial of Service).

A layer 7 protocol defence, the WAF is not designed to protect your servers against all attacks; rather, it is a part of a toolset that will ensure that you have a competent protection arsenal against the many attack vectors that form today's IT landscape.

Please think of the WAF as a sentry that sits between your web application and the Internet, accepting data and continually scanning through the data that traverses it while comparing the content against attack vector dictionaries. The EdgeWAF works with the EdgeADC providing reverse proxy and cutting-edge protection, removing threat requests before they reach the servers, and using pre-defined rules that protect your web application servers against the OWASP Top 10 threats.



How does the EdgeWAF know what to block or not?

The EdgeWAF is equipped with the latest set of ModSec rules from OWASP. These rules allow it to detect the Top 10 threats covered by the OWASP rule set. The detected threats are then displayed in the Block List by default, and the system administrator is responsible for moving any blocked items into the Whitelist as needed. The image below shows an example of threats that have been blocked.

Matched Rules	Whitelisted Rules
<ul style="list-style-type: none">920350 (Host header is a numeric IP address)930100 (Path Traversal Attack (...))930110 (Path Traversal Attack (...))930120 (OS File Access Attempt)932160 (Remote Command Execution: Unix Shell Code Found)942100 (SQL Injection Attack Detected via libinjection)942190 (Detects MSSQL code execution and information gathering attempts)949110 (Inbound Anomaly Score Exceeded (Total Score: 33))980130 (Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,I	

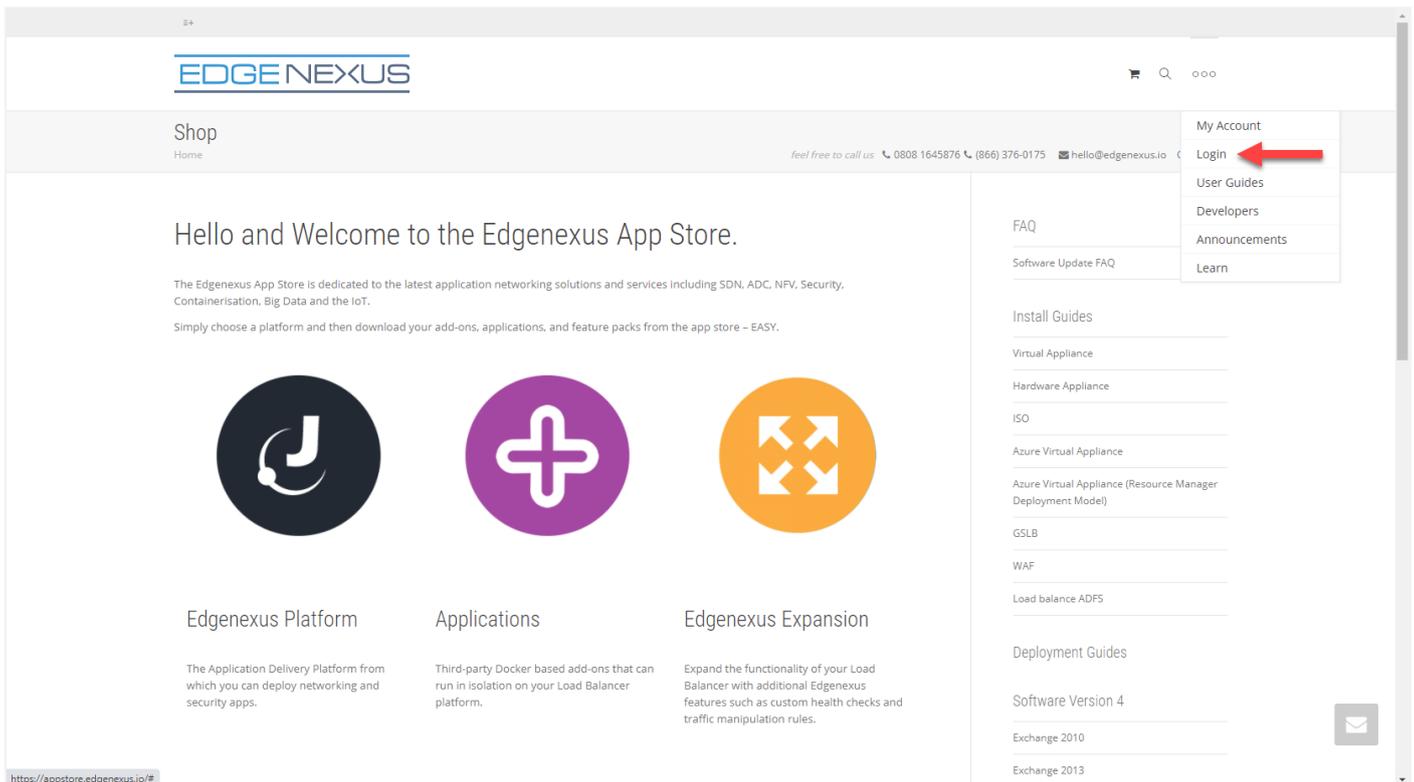
Installing the EdgeWAF App

Getting the EdgeWAF from the App Store

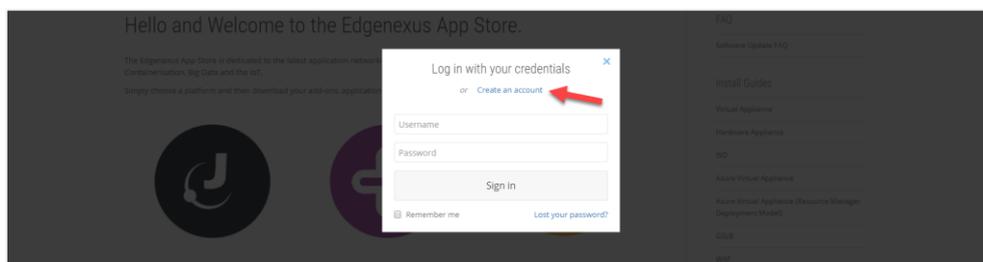
Obtaining the EdgeWAF is very easy.

As with every Edgenexus App, the EdgeWAF App is available through the App Store and is free of cost.

- The first thing to do is to register for access to the Edgenexus App Store. This process is done by using a browser and navigating to <https://appstore.edgenexus.io>.

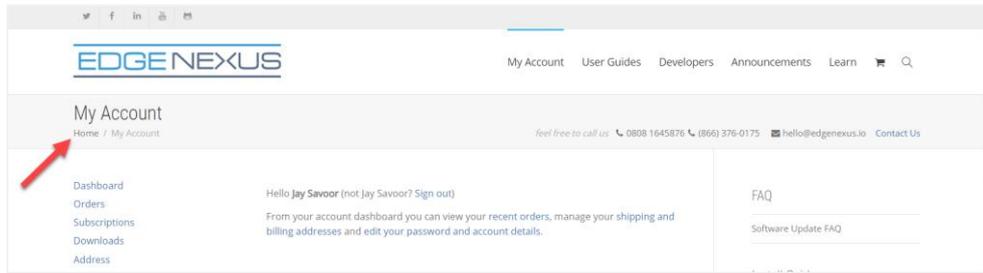


- Click on the login link in the hamburger icon at the top right.
- Click on the Create an Account, or log in using your account credentials.

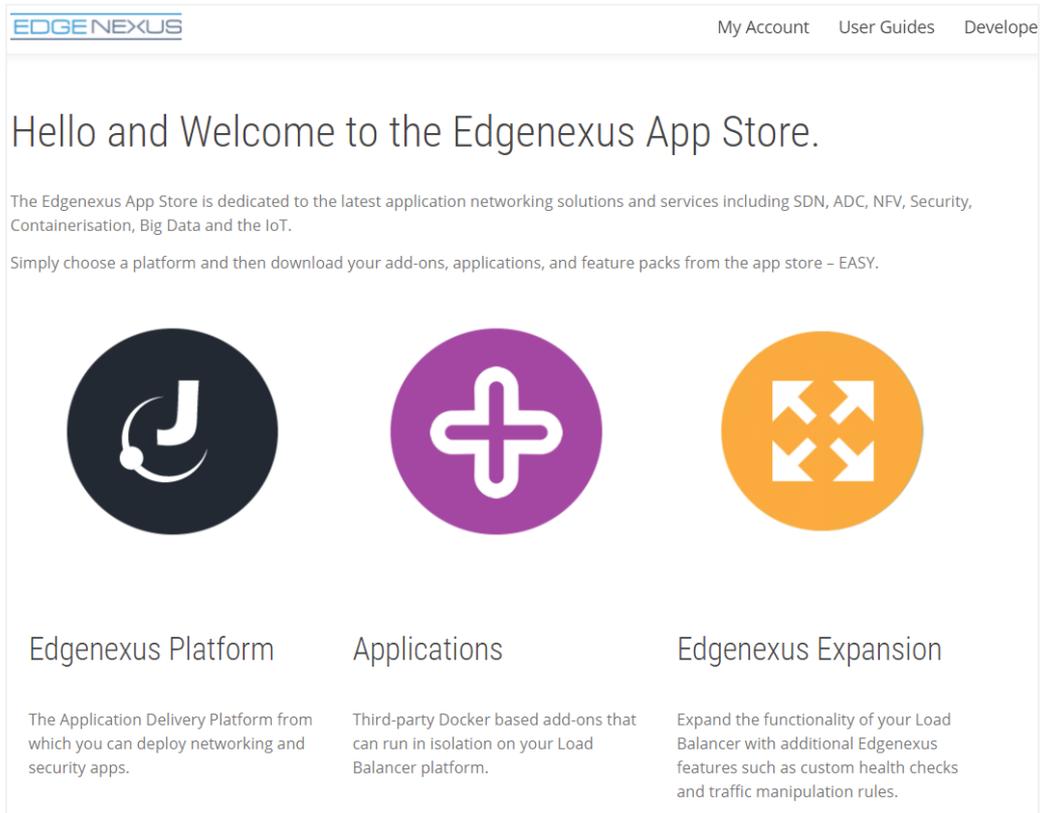


- Once you have logged in, please click on the Home link under the logo.

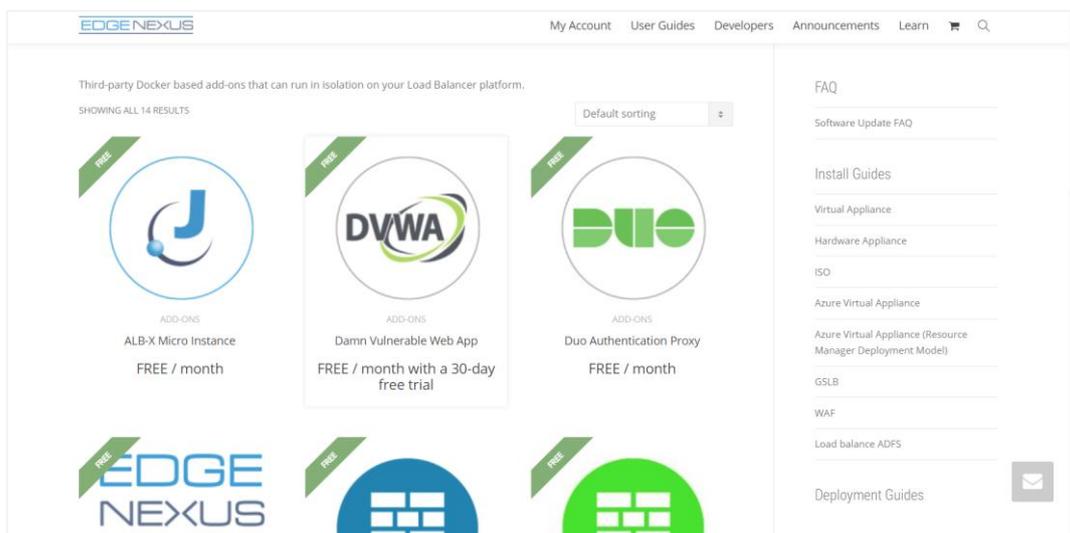
EdgeWAF Free Edition Administrator User Guide



- Next, click on Applications.



- This action will take you to the Applications page, where you can download the EdgeWAF.



- Within the applications page, you can browse for and order the App.
- The EdgeWAF is free to try, but you purchase it for full use.
- At this point, you have two options: Using the App Store from within the EdgeADC or directly downloading the App from the App Store and then uploading it to the EdgeADC.

Downloading and importing the App using the EdgeADC

- The first option is to log in using your App Store credentials inside the EdgeADC. The integrated App Store interface is available using Services > App Store.
- This method will allow you to make the purchase and then find it available within the Purchased Apps section in Library > Apps.
- EdgeWAF App looks something like the one shown below.



- You can then download the App, which will appear in the Downloaded Apps section.
- From the Library > Apps > Downloaded Apps section, locate the EdgeWAF App and then deploy it to the EdgeADC containers by clicking the Deploy button.
- Once deployed, it will be available in the Library > Add-Ons tab

Download and import the App using direct download

- The secondary method uses your App Store login and directly downloads it to your desktop using a browser.
- Once downloaded, please make sure you save it without altering the filename.
- Please also ensure that there is no (1) or something similar in the filename, possibly indicating a second download, etc.
- With the file downloaded, navigate to Advanced > Software of the EdgeADC GUI using your browser.

Making the EdgeWAF App operational

When an App is downloaded and deployed, it is yet to be operational. It has to be given an IP address in the same subnet as the EdgeADC and ports through which it needs to be accessible.

- Navigate to Library > Add-Ons and locate the EdgeWAF App.
- It should look something like the image below.

EdgeWAF Free Edition Administrator User Guide

Container - Name

Container Name:

External IP:

External Port:

Parent Image: Edgenexus-Application-Firewa

Internal IP:

Started At:

Stopped At:

Import File:

- As shown in the Container Name and External IP field, no name or IP address is allocated.
- Add an appropriate static IP address. This entry is optional for EdgeADC v4.3.x and above but is mandatory for any version lower than 4.3.x.
- Next, give the App a name – the EdgeADC's internal DNS system uses this to refer to the App when needed.

Note: The provision of a name is mandatory and essential for internal ADC <> WAF communications.

- You will need to add the relevant ports for your application, such as 80 or 443. Port 88 is required to access the EdgeWAF GUI.
- Once you have done this, click the Update button to initialise the App.
- It should look something like the one below.

Container - Name

Container Name: myWAF

External IP: 10.0.0.105

External Port: 80/tcp, 443/tcp, 88/tcp

Parent Image: Edgenexus-Application-Firewa

Internal IP:

Started At:

Stopped At:

Import File:

- Click the PLAY icon to activate the App into an operational state.

myWAF

Container Name: myWAF

External IP: 10.0.0.105

External Port: 80/tcp, 443/tcp, 88/tcp

Parent Image: Edgenexus-Application-Firewa

Internal IP: 172.31.0.17

Started At: 2023-10-20 14:27:36

Stopped At:

Import File:

Note the View App button to launch the App GUI and the Pause App and Stop App buttons.

- You can launch the App GUI using View App or the listing in the IP Services section.

The EdgeWAF App runs within the ADC's docker container technology, ensuring its safety and integrity. The App uses a separate docker0 network to communicate with the EdgeADC load balancer. When the App is started, it is allocated an IP address from the docker0 pool. This IP address is automatically resolved by the EdgeADC using the docker name you provided in the Container Name field. You can see the internal IP address on the right side of the App.

Using the EdgeWAF

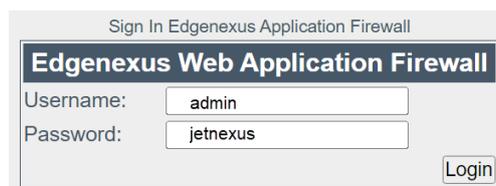
To configure and use the EdgeWAF, you must access it via the EdgeADC or a web browser if you have installed it onto an EADP (Edgenexus Application Delivery Platform) system.

If installed within the EdgeADC, please click the Add-on GUI button as seen in the image below.



Otherwise, use the URL via a web browser. An example of this would be <https://192.168.159.122:88>, where the IP address within the URL matches the value of the External IP you provided.

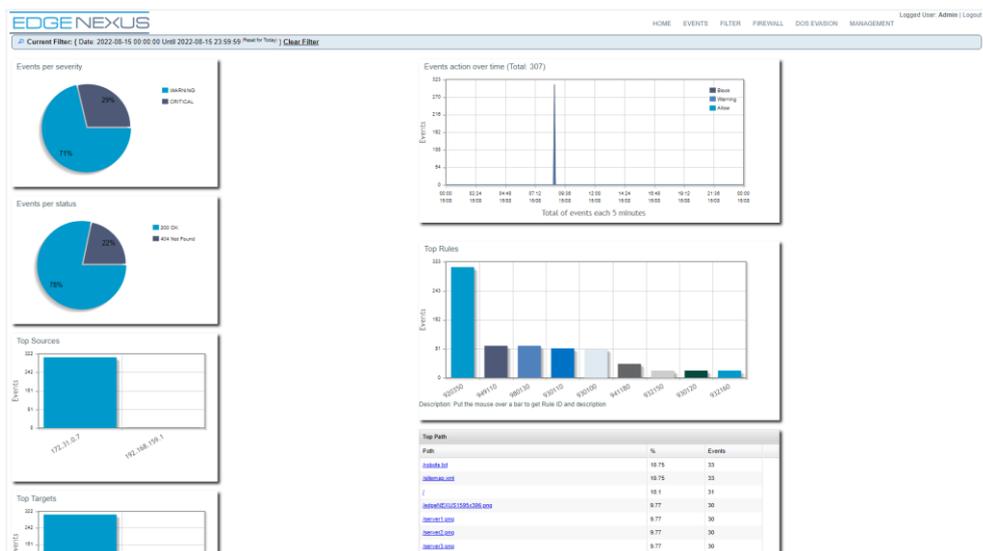
You will now be presented with a login prompt like the example below.



The default credentials are shown in the image above.

Once logged in, you will be presented with the Dashboard.

The Dashboard



As you can see from the image above, a menu and several graphs and tables are shown in the Dashboard. The menu allows you to navigate through the different pages of the EdgeWAF administration system, while the graphs and tables represent the events detected by the EdgeWAF and classified by numerous parameters.

The Events Page

Event	Action	Sensor	Severity	Date/Time	Source/Port	Hostname/Path	Rules Alert
Details	WAF	WAF	Warning	2022-08-15 08:47:32	172.31.0.7 38332	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /admin/, Status Code: 404 (Not Found)	Host header is a numeric IP address (192.168.159.114)
Details	WAF	WAF	Warning	2022-08-15 08:47:32	172.31.0.7 38332	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server6.png? query=%7C Status Code: 200 (OK)	Host header is a numeric IP address (192.168.159.114)
Details	WAF	WAF	Warning	2022-08-15 08:47:32	172.31.0.7 38332	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server6.png? query=%00 Status Code: 200 (OK)	Invalid character in request (null character) (REQUEST_URI=/server6.png? query=%00) Invalid character in request (null character) (ARGS=query=%00) Inbound Anomaly Score Exceeded (Total Score: 33) Host header is a numeric IP address (192.168.159.114) Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,RFI=0,LF=30,RCE=0,PHPI=0,HTTP=0,SESS=0), individual paranoia level scores: 33, 0, 0, 0
Details	WAF	WAF	Warning	2022-08-15 08:47:32	172.31.0.7 38332	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server6.png? query=%2B Status Code: 200 (OK)	Host header is a numeric IP address (192.168.159.114)
Details	WAF	WAF	Warning	2022-08-15 08:47:32	172.31.0.7 38332	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server6.png? query=%40 Status Code: 200 (OK)	Host header is a numeric IP address (192.168.159.114)
Details	WAF	WAF	Warning	2022-08-15 08:47:32	172.31.0.7 37228	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server6.png? query= Status Code: 200 (OK)	Host header is a numeric IP address (192.168.159.114)
Details	WAF	WAF	Warning	2022-08-15 08:47:32	172.31.0.7 37228	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server6.png? query= Status Code: 200 (OK)	Host header is a numeric IP address (192.168.159.114)

The Events page within the EdgeWAF displays the events detected by the EdgeWAF. The log of events comprises descriptive text and hot links that will show more detailed data.

If we look at a single event line, for example, we can interrogate the system for more information or filter the records according to the event type.

Details	WAF	WAF	Warning	2022-08-15 08:47:32	172.31.0.7 38332	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server6.png? query=%00 Status Code: 200 (OK)	Invalid character in request (null character) (REQUEST_URI=/server6.png? query=%00) Invalid character in request (null character) (ARGS=query=%00) Inbound Anomaly Score Exceeded (Total Score: 33) Host header is a numeric IP address (192.168.159.114) Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,RFI=0,LF=30,RCE=0,PHPI=0,HTTP=0,SESS=0), individual paranoia level scores: 33, 0, 0, 0
-------------------------	-----	-----	---------	---------------------	---------------------	--	--

If we were to click on the link Details, we would be presented with a detailed view of what this event comprises. See below:

Rules Match	Message	Transaction ID
920270	Rule Message: Invalid character in request (null character) Event: Found 1 byte(s) in REQUEST_URI outside range: 1-255 Data: REQUEST_URI=/server6.png?query=%00 Tags: application-multi language-multi platform-multi attack-protocol paranoia-level/1 OWASP_CRS capec/1000/210/272	2425
920270	Rule Message: Invalid character in request (null character) Event: Found 1 byte(s) in ARGS:query outside range: 1-255 Data: ARGS=query=%00 Tags: application-multi language-multi platform-multi attack-protocol paranoia-level/1 OWASP_CRS capec/1000/210/272	WAF
949110	Rule Message: Inbound Anomaly Score Exceeded (Total Score: 33) Event: Operator GE matched 5 at TX.anomaly_score Tags: application-multi language-multi platform-multi attack-generic	Unique ID Yv0JHsCCVcdLWjInEbXsQAA
920350	Rule Message: Host header is a numeric IP address Event: Pattern match "%[0-9]+%" at REQUEST_HEADERS:Host Data: 192.168.159.114 Tags: PCIS.5.10 application-multi language-multi platform-multi attack-protocol paranoia-level/1 OWASP_CRS capec/1000/210/272	Action Warning
980130	Rule Message: Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,RFI=0,LF=30,RCE=0,PHPI=0,HTTP=0,SESS=0), individual paranoia level scores: 33, 0, 0, 0 Event: Operator GE matched 5 at TX.inbound_anomaly_score event-correlation	Engine Mode DETECTION_ONLY (modsecurity 2.7+ only)

Request Details	Performance
GET /server6.png?query=%00 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0 Cache-Control: no-cache Content-Length: 0 Referer: http://192.168.159.114 Content-Length: 0 Referer: http://192.168.159.114 Host: 192.168.159.114	Duration: 5.417 msec Combined: 1.25 msec Phase 1: 0.353 msec Phase 2: 0.644 msec Phase 3: 0.033 msec Phase 4: 0.095 msec Phase 5: 0.124 msec Storage read: 0.091 msec Storage write: 0.001 msec Logging: 0 msec Garbage collection: 0 msec

Response Details	Server
HTTP/1.1 200 OK Content-Type: image/png Last-Modified: Fri, 28 Apr 2017 09:55:40 GMT Accept-Ranges: bytes	Apache/2.4.6 (CentOS) PHP/5.4.16 ModSecurity for Apache/2.9.2 (http://www.modsecurity.org/) OWASP_CRS/3.2

If, however, we were to click on the line stating:

Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,RFI=0,LFI=30,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 33, 0, 0, 0

The Events list will be filtered to show all events corresponding to the clicked value.

The screenshot shows the EdgeWAF Events list with a filter applied. The filter is 'Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,RFI=0,LFI=30,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 33, 0, 0, 0'. The table displays four events, all with a severity of 'High' and a status of 'OK'. The events are filtered by the selected rule ID (980130).

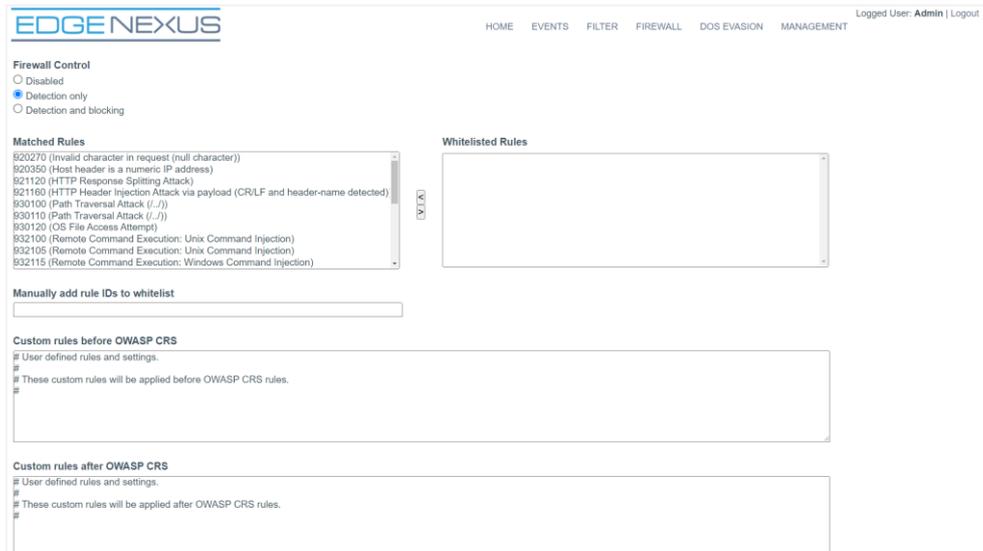
Event	Action	Sensor	Severity	Date/Time	Source/Port	Hostname/Path	Rules Alert
<input type="checkbox"/>	Details	WAF	High	2022-08-15 08:47:32	172.31.0.7 38332	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server6.png?query=i%00 Status Code: 200 (OK)	Invalid character in request (null character) (REQUEST_URI=/server6.png?query=i%00) Invalid character in request (null character) (ARGS=query=i%00) Inbound Anomaly Score Exceeded (Total Inbound Score: 33) Host header is a numeric IP address (192.168.159.114) Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,RFI=0,LFI=30,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 33, 0, 0, 0
<input type="checkbox"/>	Details	WAF	High	2022-08-15 08:47:32	172.31.0.7 37592	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server5.png?query=i%00 Status Code: 200 (OK)	Invalid character in request (null character) (REQUEST_URI=/server5.png?query=i%00) Invalid character in request (null character) (ARGS=query=i%00) Inbound Anomaly Score Exceeded (Total Inbound Score: 33) Host header is a numeric IP address (192.168.159.114) Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,RFI=0,LFI=30,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 33, 0, 0, 0
<input type="checkbox"/>	Details	WAF	High	2022-08-15 08:47:31	172.31.0.7 37228	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server4.png?query=i%00 Status Code: 200 (OK)	Invalid character in request (null character) (REQUEST_URI=/server4.png?query=i%00) Invalid character in request (null character) (ARGS=query=i%00) Inbound Anomaly Score Exceeded (Total Inbound Score: 33) Host header is a numeric IP address (192.168.159.114) Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,RFI=0,LFI=30,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 33, 0, 0, 0
<input type="checkbox"/>	Details	WAF	High	2022-08-15 08:47:31	172.31.0.7 37592	Hostname: 192.168.159.114, Port: 80, Method: GET, Path: /server3.png?query=i%00	Invalid character in request (null character) (REQUEST_URI=/server3.png?query=i%00)

The Filter Editor

The Filter Editor allows you to filter displayed events with even greater granularity.

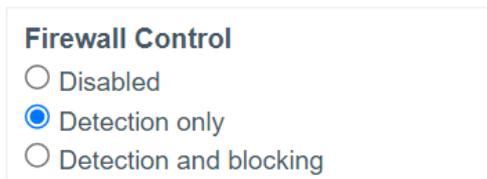
The Filter Editor dialog box is open, showing various filtering options. The 'General' tab is selected, and the 'Date From' and 'Date To' fields are set to 2022-08-15 00:00:00 and 2022-08-15 23:59:59 respectively. The 'Sensor' is set to 'All Sensors', and the 'Action' is set to 'All Actions'. The 'Event Severity' is set to 'All Severities'. The 'Engine Mode' is set to 'All'. The 'HTTP Method' is set to 'All Method'. The 'Path' is set to 'All Status'. The 'User ID', 'Rule ID', 'Tag', 'Web App Info', 'Marked as False Positive', 'Preserved Events', and 'Unique ID' fields are empty. The 'Anomaly Scoring' section has 'Total Score', 'SQLi Score', and 'XSS Score' set to '≥'. The 'Rule Timing (in milliseconds)' section has 'Duration', 'Combined', 'Phase 1', 'Phase 2', 'Phase 3', 'Phase 4', 'Phase 5', 'Storage Read', 'Storage Write', 'Logging', and 'Garbage Collection' set to '≥'. The 'Apply Filter', 'Cancel', and 'Clear Filter' buttons are visible at the bottom.

Firewall

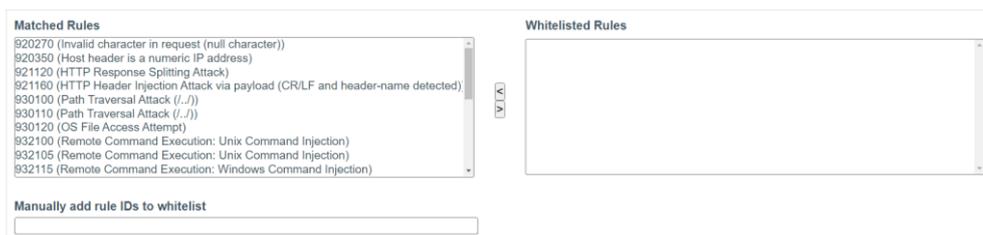


The Firewall page is a critical section of the EdgeWAF and is used to ensure that you first scan the traffic without blocking and then whitelist the safe events before switching to block mode.

Firewall Control



- **Disabled** – the WAF is disabled and allows all traffic to pass through without detection.
- **Detection only** – In this mode, the WAF will detect all events that conform to the OWASP rule set and list them. It will not block any traffic. This mode is used to understand the traffic coming through the WAF and the effect blocking certain events may have.
- **Detection and blocking** – This is the fully operational mode, and when set to this option, the WAF will block all events not whitelisted.



The *Manually add rule IDs to whitelist* option allows you to add additional rules using their IDs to the whitelist section.

DoS Evasion

The screenshot shows the 'EDGE NEXUS' web interface with the 'DOS EVASION' tab selected. The 'DoS Evasion Control' section has 'Disabled' selected. The 'DoS Evasion Parameters' section includes input fields for: DOS Hash Table Size (3097), DOS Page Count (2), DOS Site Count (50), DOS Page Interval (1), DOS Site Interval (1), and DOS Blocking Period (10). There is a checked checkbox for 'Use IPTables for blocking' and an input field for 'IPTables Blocking Period' (1). The 'DoS Evasion IP Whitelist' section contains a text area with a sample configuration: '# You can use whitelists to disable the module for certain ranges of # IPs. Wildcards can be used on up to the last 3 octets if necessary. # Multiple DOSWhitelist commands may be used in the configuration. #DOSWhitelist: 192.168.0.* #'. An 'Update configuration' button is at the bottom.

Denial of Service attacks is more prevalent these days than ever before. The DoS Evasion capability of the EdgeWAF system allows you to decrease the risk by enabling DoS attack prevention.

You can specify custom properties using the DoS Evasion Parameters section and provide IP addresses considered safe within the DoS Evasion IP Whitelist section.

Management

The Management section of the EdgeWAF configuration allows you to set additional parameters and users that are permitted to log into the EdgeWAF web console.

The screenshot shows the 'EDGE NEXUS' web interface with the 'MANAGEMENT' tab selected. The left navigation menu has 'Config', 'Users', and 'Info' options. The main content area is titled 'Real Server / VIP' and includes: a text input for 'Real Server / VIP Address' (192.168.159.115); 'Requests Keep-Alive' with 'Disabled' selected; 'Proxy Preserve Host' with 'Enabled' selected; 'Absolute URL to Relative URL' with a text input; 'Client IPs Forwarding' with a text input; and 'Log Storage' with 'Store Local Logs' checked and 'Store Remote Logs' unchecked. An 'Update configuration' button is at the bottom.

Management Navigation Menu

At the top left of the management page, you will find the menu that allows you to navigate the various sections.

These are:

- [Config](#)

- Users
- Info.

Config

The Config section enables the admin to set various parameters that govern the behaviour of the EdgeWAF.

Real Server / VIP
Real Server / VIP Address

Requests Keep-Alive
 Enabled
 Disabled

Proxy Preserve Host
 Enabled
 Disabled

Absolute URL to Relative URL
Convert specified absolute URL to a relative URL in response body (strip host address part of the URL)

Client IPs Forwarding
Get client IPs from "X-Forwarded-For" header generated by a reverse proxy at the following IP address

Log Storage
 Store Local Logs
 Store Remote Logs

Item	Description
Real Server / VIP	This field allows you to specify to which server or ADC VIP the EdgeWAF will send egress data once traffic detection and blocking are completed.
Requests Keep-Alive	Allows you to enable or disable the Keep-Alive timeout associated with requests
Proxy Preserve Host	The Proxy Preserve Host setting, when enabled, allows the preservation and retention of the original Host: header from the client browser when constructing the proxied request to send to the target server.
Absolute URL to Relative URL	This option allows the removal of the host information from the URL. So http://test.com/home becomes /home.
Client IPs forwarding	Obtains the client's IP address from the X-Forwarded-For header generated by the reverse proxy at the specified address.
Log Storage	Choose whether to store the logs locally or in a remote location.

Users

The EdgeWAF allows you to create specific user logins. This feature is accessed using the Users menu item on the Management page.

EdgeWAF Free Edition

Administrator User Guide



In this section, you can see the users that have been defined and edit existing ones and change the password for a specific user.

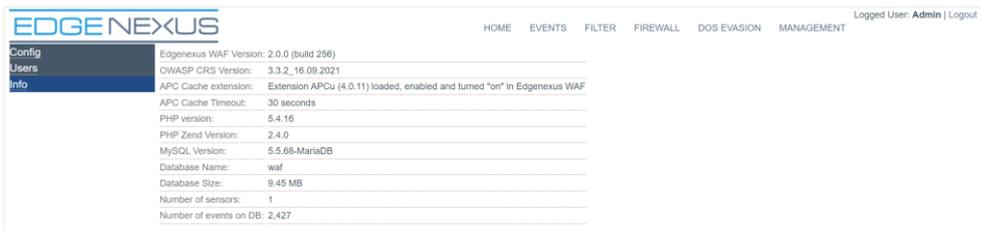
To add a new user, click the Add New User button. You will see the page below.

Username (Min. 5 - Max. 30 characters)
Password (Min. 5 - Max. 20 characters)
Password (confirmation) (Min. 5 - Max. 20 characters)
e-mail

Enter the details and click save.

Info

Should you wish to obtain information on the version number of the WAF and any other related information, click Info.

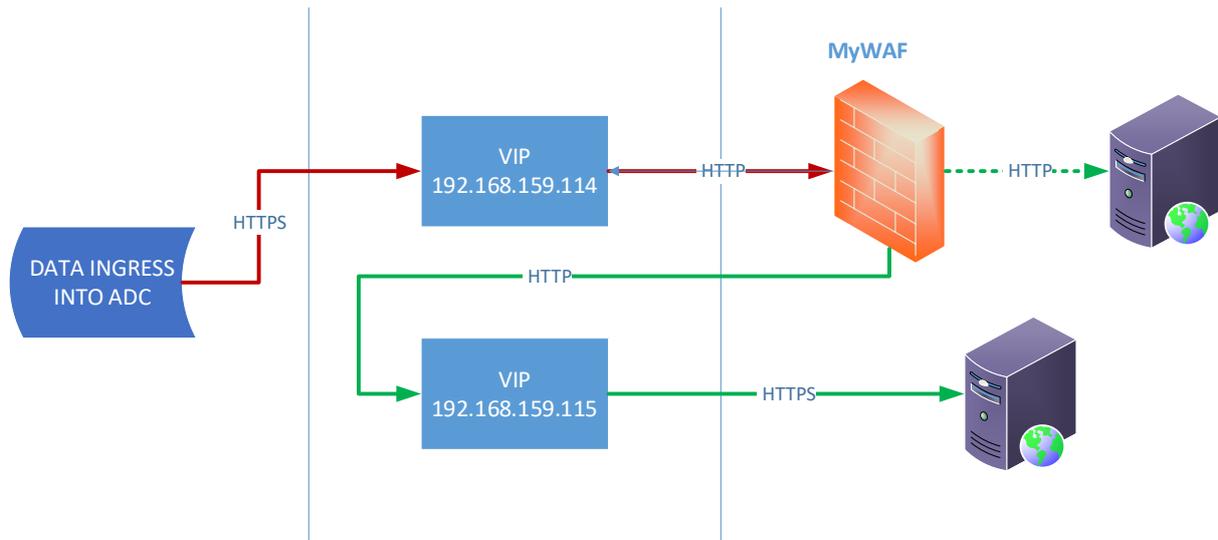


How to use the EdgeWAF

The EdgeWAF is available for use within two platforms:

- EdgeADC – Installed locally within the EdgeADC as a containerised application
- EADP (Edgenexus Application Delivery Platform) – The EADP platform allows you to host Edgenexus as standalone systems where you may be using a 3rd party load balancer or no load balancer at all.

In this example of how to use the WAF in a real scenario, we will use the EdgeADC. Operationally, there is no difference, and the egress IP will point to a VIP rather than a real server.



As we can see from the diagram above, data ingress occurs to the VIP 192.168.159.114 and is then sent onto the WAF. You will need to configure for SSL offload if the traffic is HTTPS – set the port for the ingress VIP to 443 and the port for WAF entry to 80 (our example).

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			<input checked="" type="checkbox"/>	192.168.159.115	255.255.255.0	443	From WAF	HTTP
Active			<input checked="" type="checkbox"/>	192.168.159.114	255.255.255.0	443	MAIN INGRESS	HTTP
Active			<input checked="" type="checkbox"/>	192.168.159.116	255.255.255.0	80	Paul	HTTP
Active			<input checked="" type="checkbox"/>	192.168.159.117	255.255.255.0	80	John	HTTP
Active			<input checked="" type="checkbox"/>	192.168.159.118	255.255.255.0	80	Ringo	HTTP
Active			<input checked="" type="checkbox"/>	192.168.159.119	255.255.255.0	80	gsibjayadc.com	HTTP
Active			<input checked="" type="checkbox"/>	192.168.159.120	255.255.255.0	80	gsibjayadc.com	HTTP

Server	Basic	Advanced	flightPATH				
Group Name: Server Group							
Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
Online		MyWAF	80	100	100		

Once tested for threats, the data egresses from the WAF to the secondary VIP 192.168.159.115 and is then sent to the real server. The IP address 192.168.159.115 is entered in the Real Server/VIP field on the WAF, as illustrated in the image below.

Real Server / VIP
Real Server / VIP Address

Using this method, you will decrypt the HTTPS traffic to the WAF and then re-encrypt the traffic onto the real server.

We have also shown how you can send the data directly to a real server in non-encrypted format (see dotted green line).