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

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

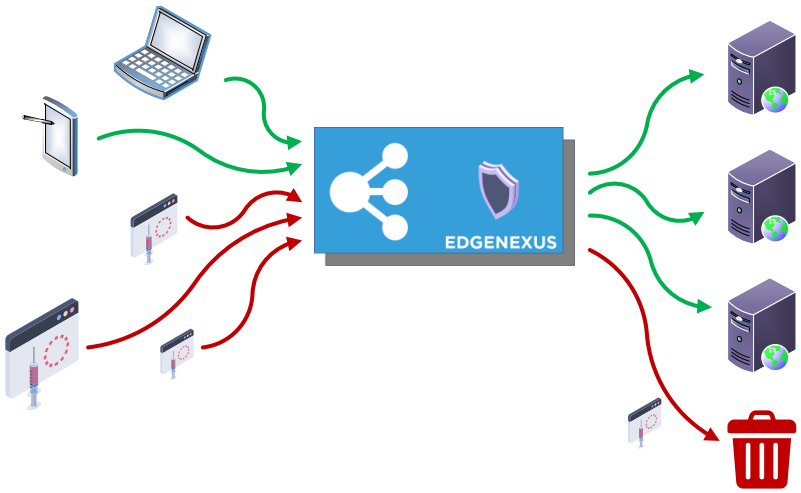
WAF Explained

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.

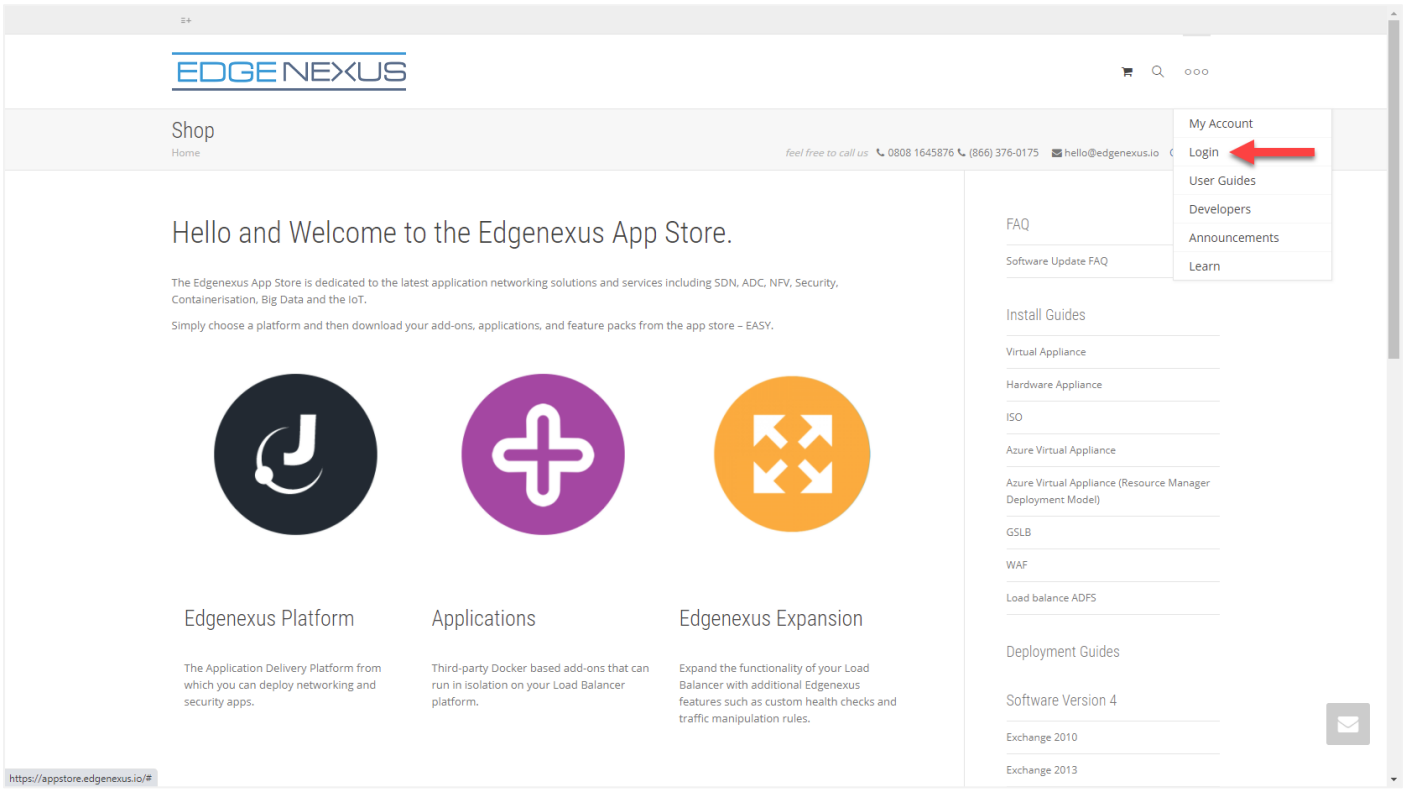
Installing the EdgeWAF App

Getting the EdgeWAF from the App Store

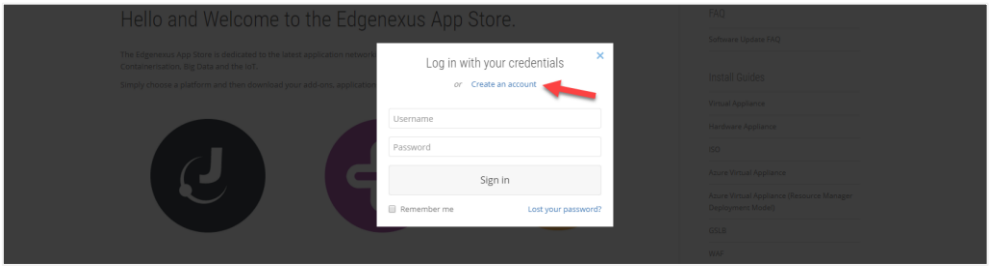
Obtaining the EdgeWAF is very easy.

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

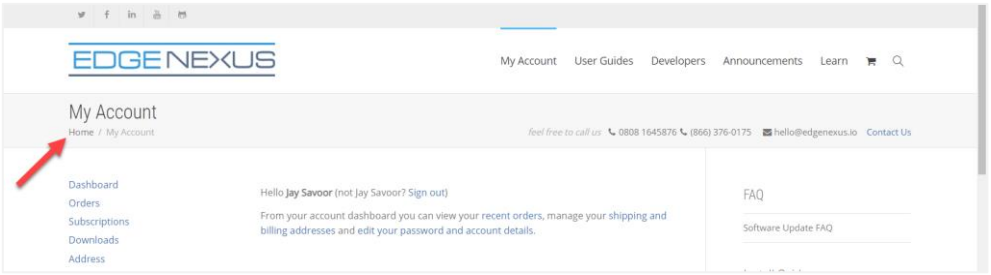
- The first thing to do is to register for access to the Edgenexus App Store. This process is done by using a browser and navigating to https://appstore.edgenexus.io.



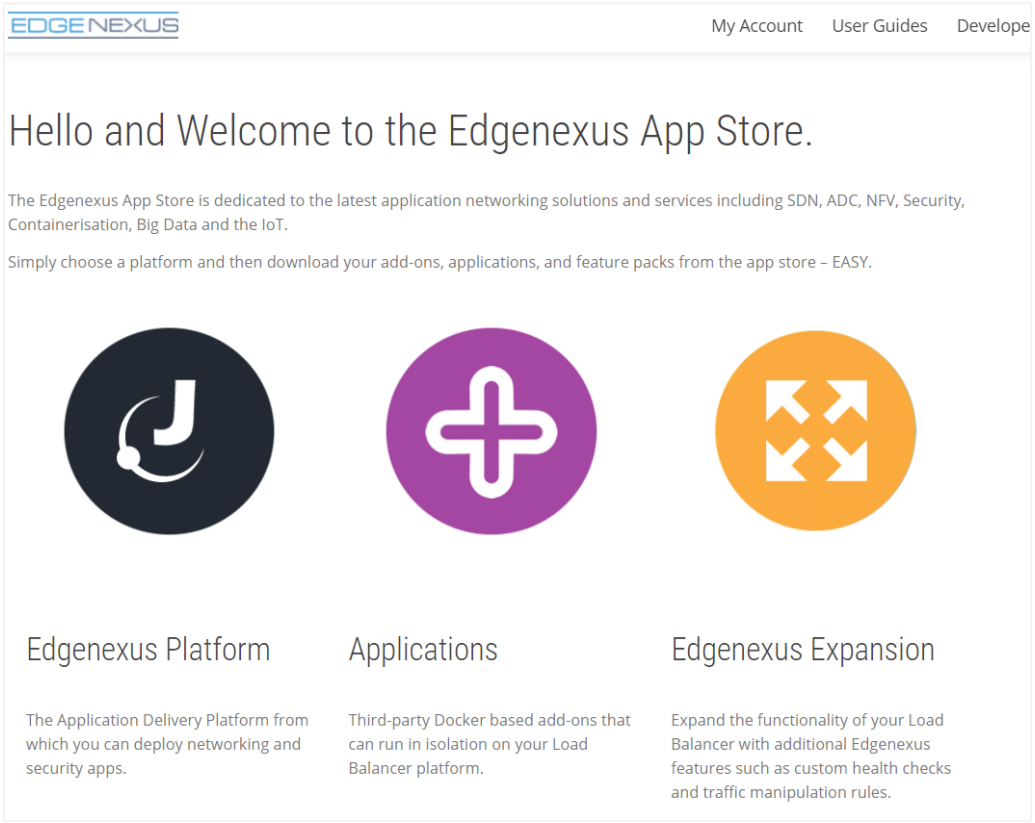
- Click on the login link in the hamburger icon at the top right.
- Click on the Create an Account, or log in using your account credentials.



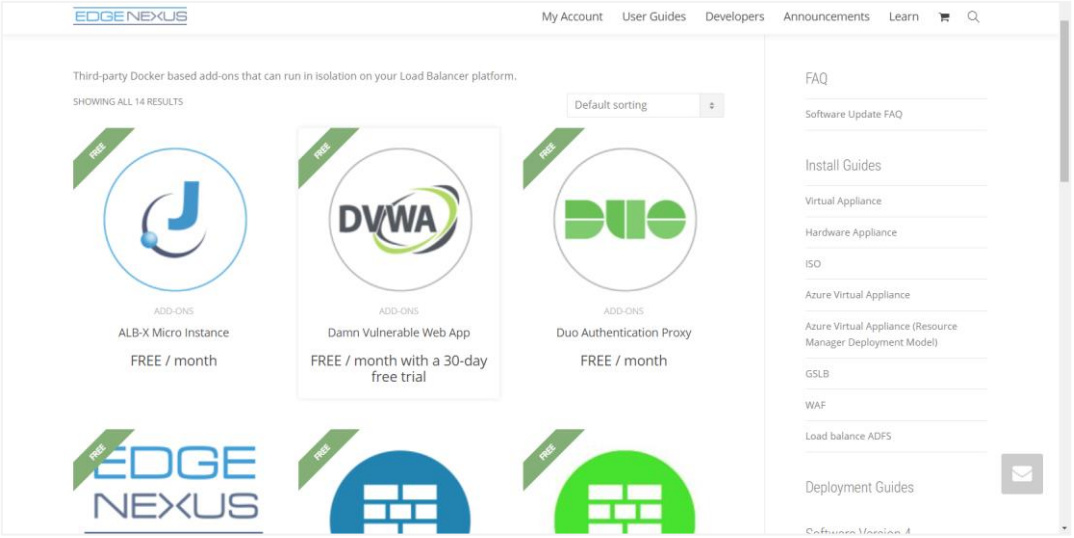
- Once you have logged in, please click on the Home link under the logo.



- 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

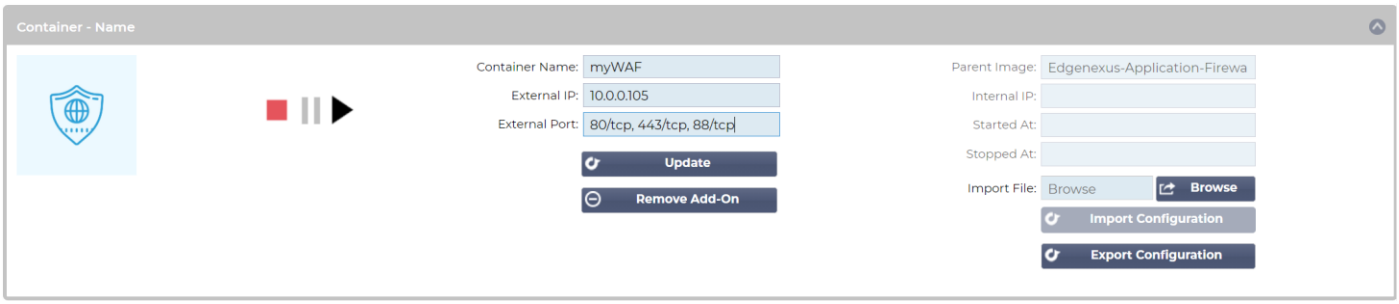
When an App is downloaded and deployed, it is yet to be operational. It has to be given an IP address in the same subnet as the EdgeADC and ports through which it needs to be accessible.

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

- 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.



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

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.

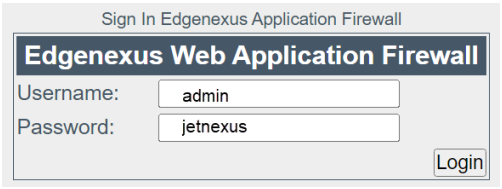
Using the EdgeWAF

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.

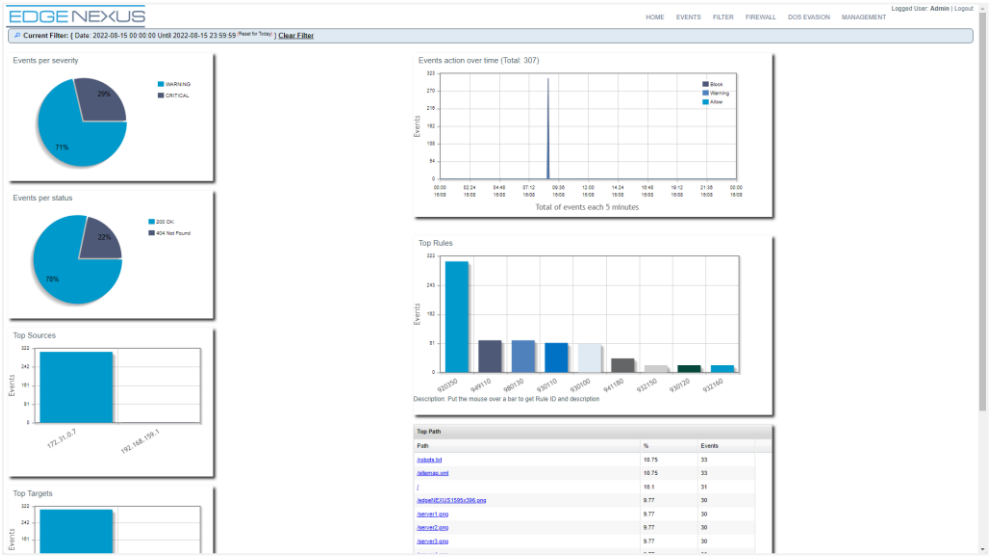
You will now be presented with a login prompt like the example below.



The default credentials are shown in the image above.

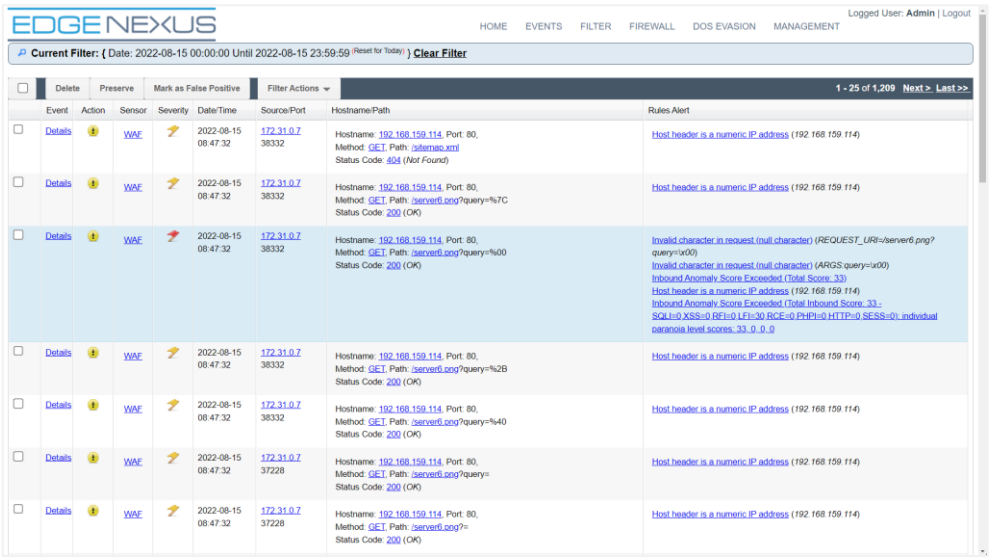
Once logged in, you will be presented with the Dashboard.

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.

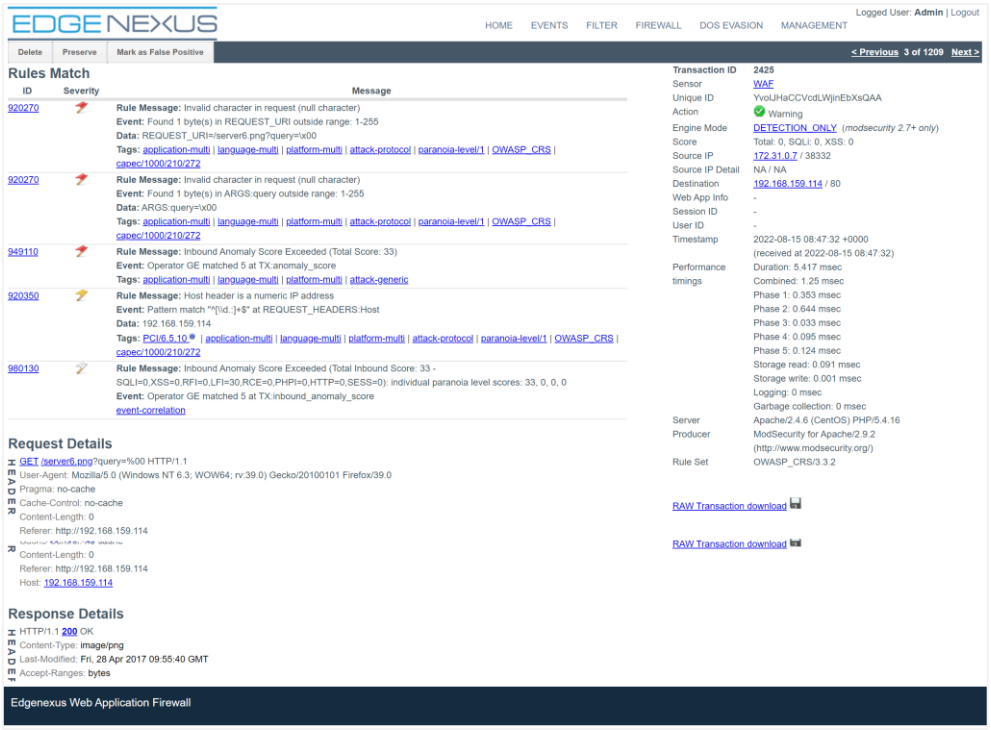
The Events Page



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.

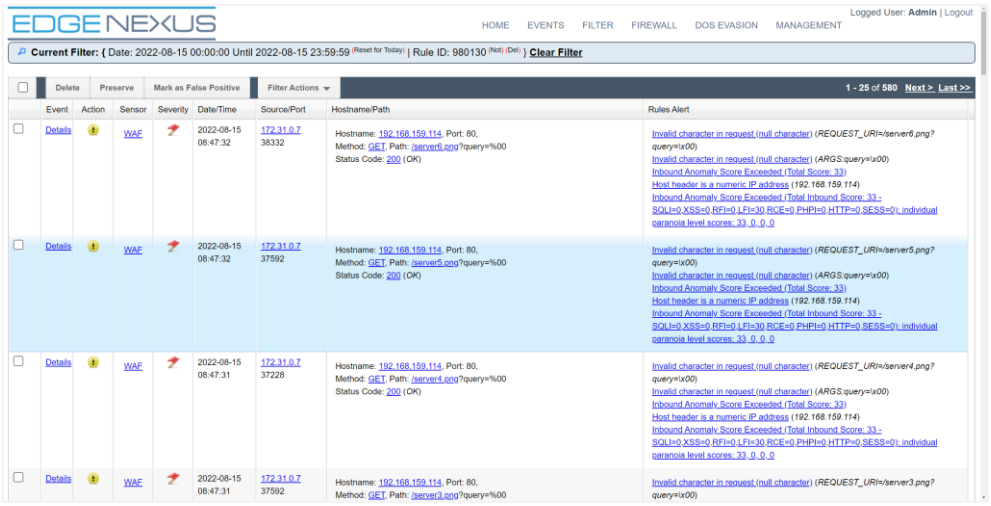
If we were to click on the link Details, we would be presented with a detailed view of what this event comprises. See below:



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

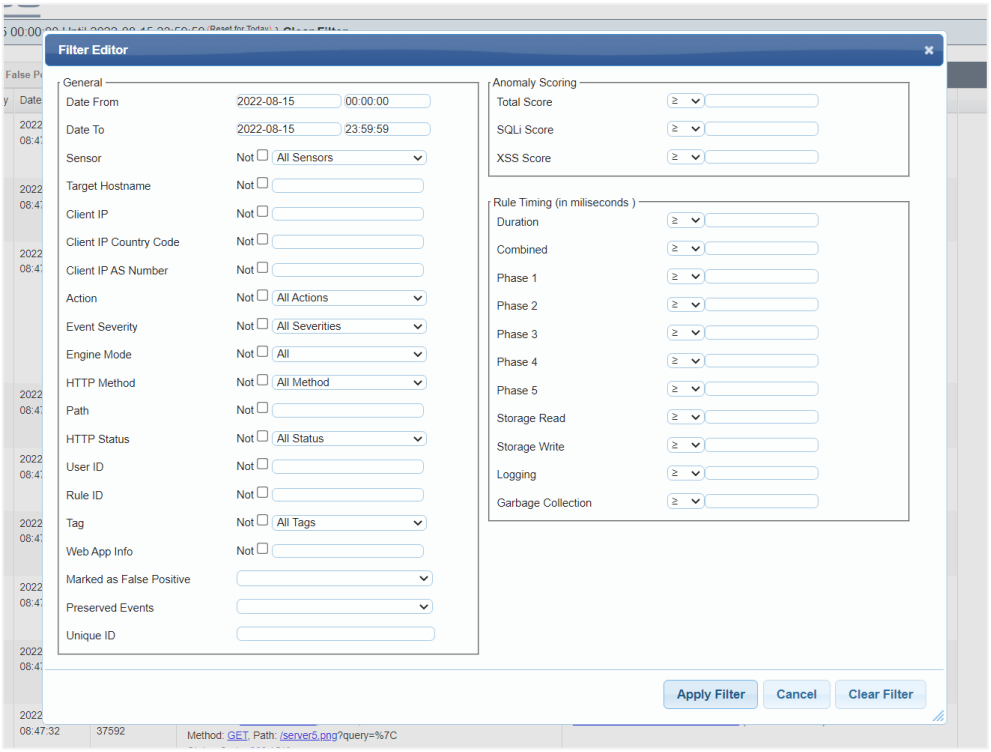
> Inbound Anomaly Score Exceeded (Total Inbound Score: 33 - SQLI=0,XSS=0,RFI=0,LFI=30,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 33, 0, 0, 0

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

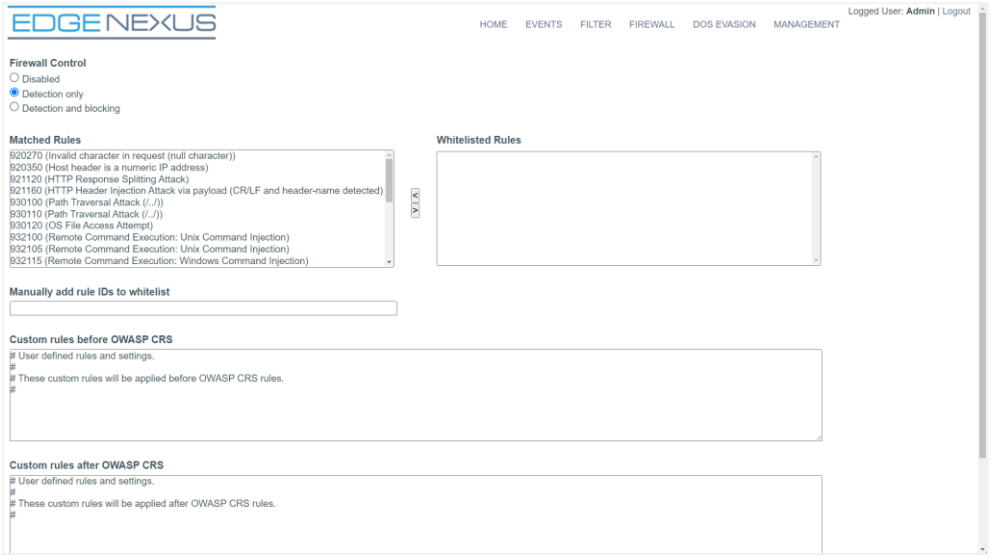


The Filter Editor

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

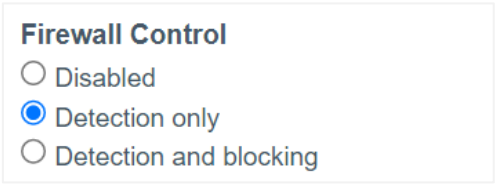


Firewall



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.

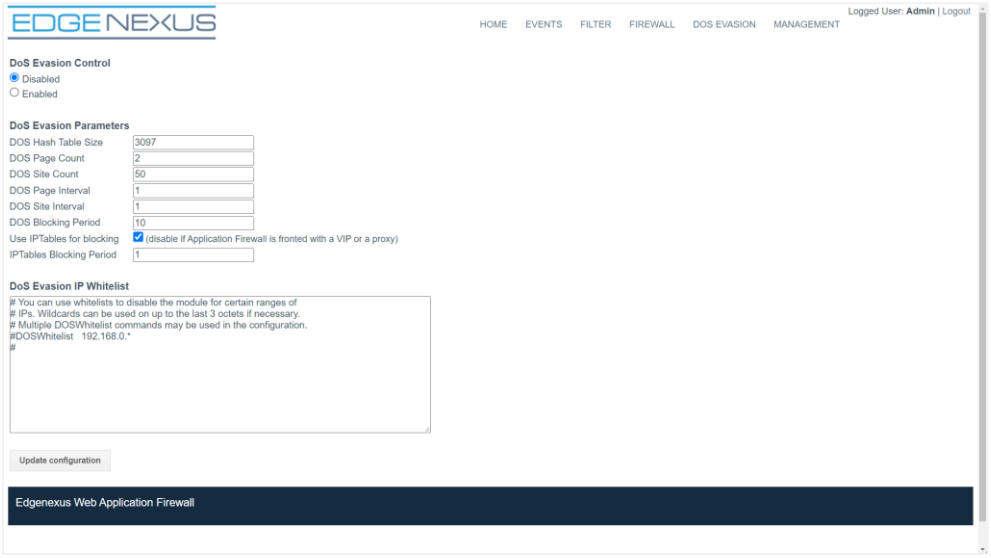
Firewall Control



- 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

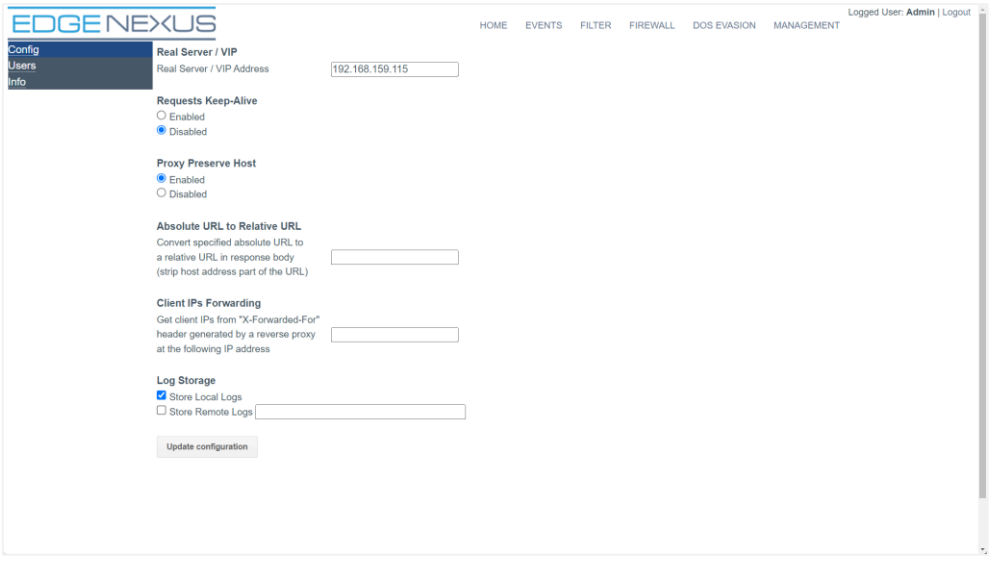


Denial of Service attacks is more prevalent these days than ever before. The DoS Evasion capability of the EdgeWAF system allows you to decrease the risk by enabling DoS attack prevention.

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.



Management Navigation Menu

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

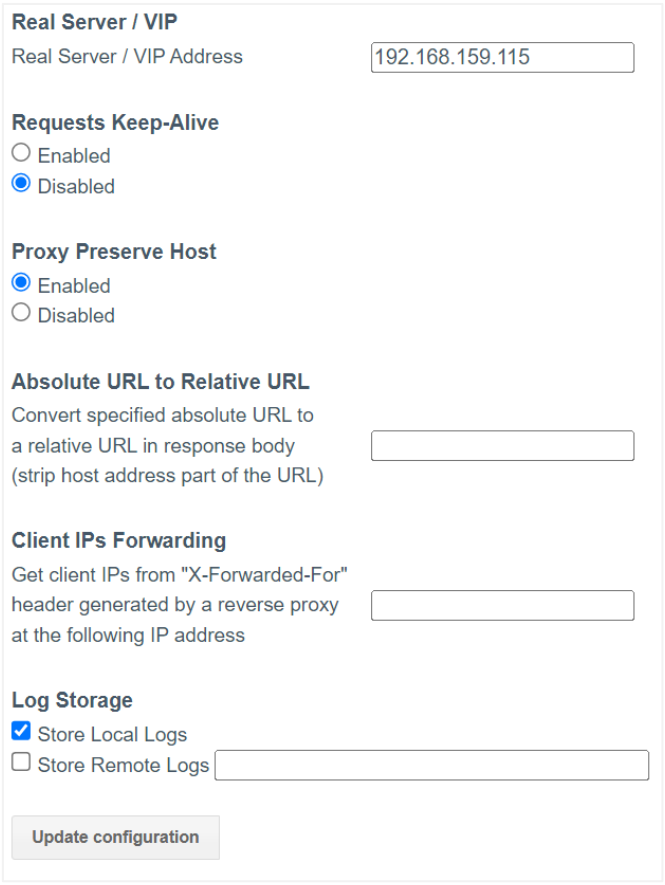
These are:

- Config

- Users
- Info.

Config

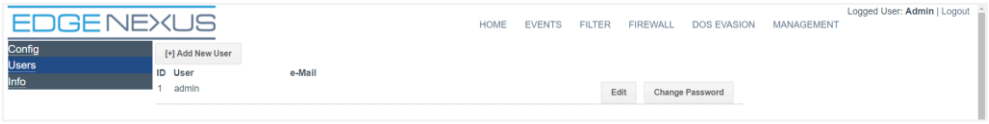
The Config section enables the admin to set various parameters that govern the behaviour of the EdgeWAF.



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.



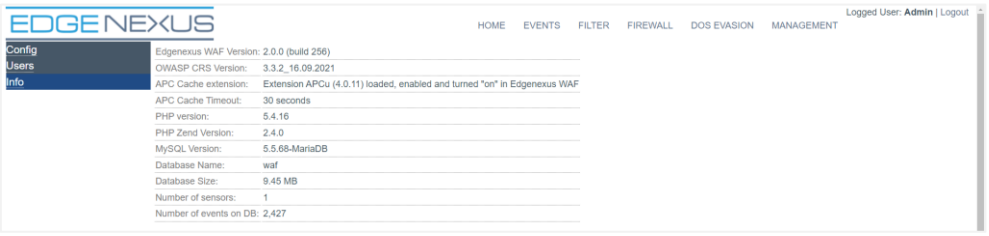
In this section, you can see the users that have been defined and edit existing ones and change the password for a specific user.

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

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.

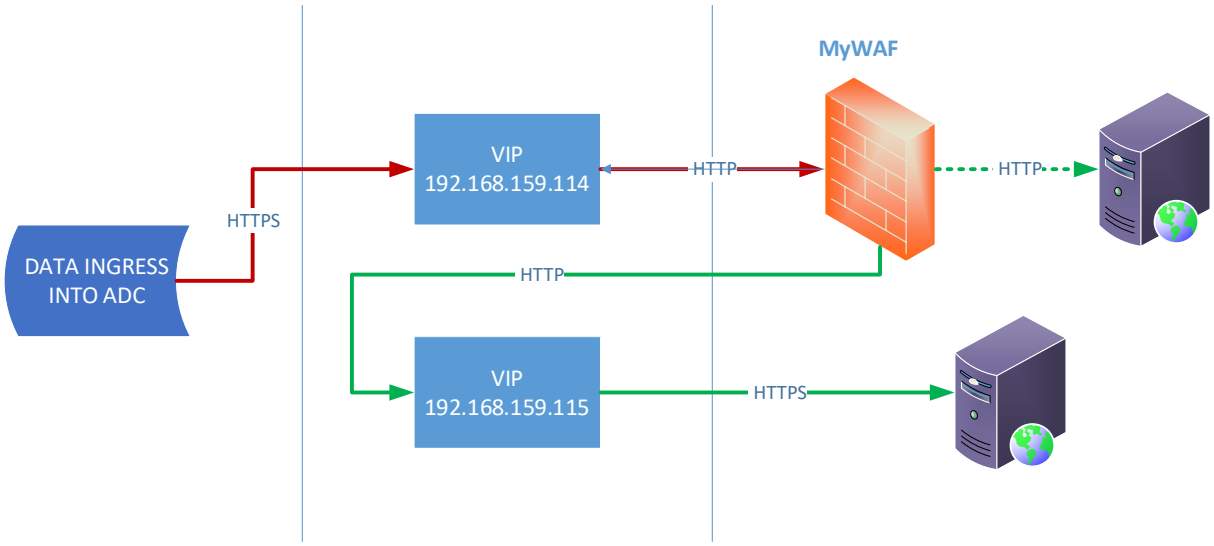


How to use the EdgeWAF

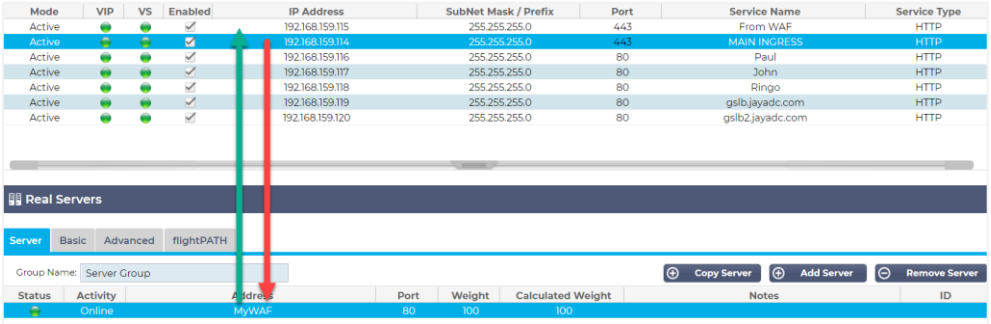
The EdgeWAF is available for use within two platforms:

- 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).



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.

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).