User Manual

Document Control	
Reference	MS_SB/MAN/001
Distribution	Standard
Status	Approved
Version	1.1
Date	01st Sept 2021

About StrongBox IT

StrongBox IT was founded with the purpose of providing confidence to the businesses against all operational failures. Our vision is to help people and enterprises StrongBox their IT infrastructure in terms of security, performance, Continuous regression, scalability and availability.

Today's production environment is a conduit of varied technologies trying to interact as one unified system. This pushes the operational support team to scale, at times, beyond their capacity to ensure continuous availability of business systems. StrongBox IT compliments the operational support team in their endeavor by helping them validate every change being rolled into production

To address the need of protecting business from IT downtime, StrongBox IT provides security testing, performance testing and regression automation services.

Contents

Where do we stand in the world of internet and innovation?

Accelerated digital innovation is a double-edged sword that hangs over the cybersecurity threat landscape. As companies rapidly pursue digital transformation to compete, they can expose more of their business to cyber disruption and theft. The problem is that cyber criminals are innovating in lockstep or, in some cases, at a greater rate.

It's easy to take your eye off the ball given the complexity in both technology innovation and the cybersecurity threat landscape. It's more important than ever to ensure a continued focus on your cybersecurity strategic plan, making adjustments based on the evolving threat landscape so that you are prepared to prevent, detect, and remediate cybersecurity issues.

If this can be achieved by a simple 10-minute process, why wait. Channel years of cybersecurity experience, collective intelligence of world's leading experts and a time-tested product to protect your information and data assets.

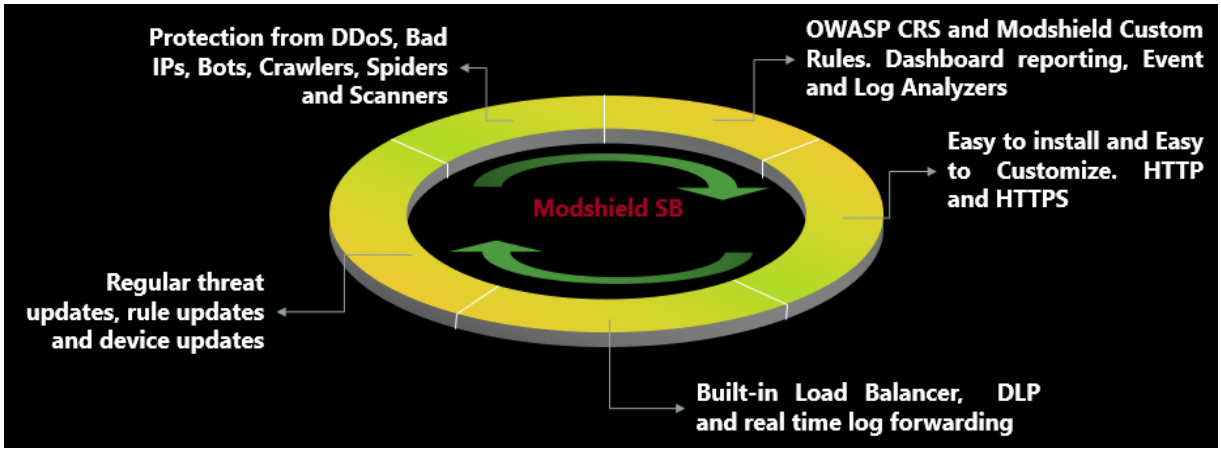
Web Application Firewall – A Quick Introduction

A web application firewall (or WAF) filters, monitors, and blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that a WAF is able to filter the content of specific web applications while regular firewalls serve as a safety gate between servers. By inspecting HTTP traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.

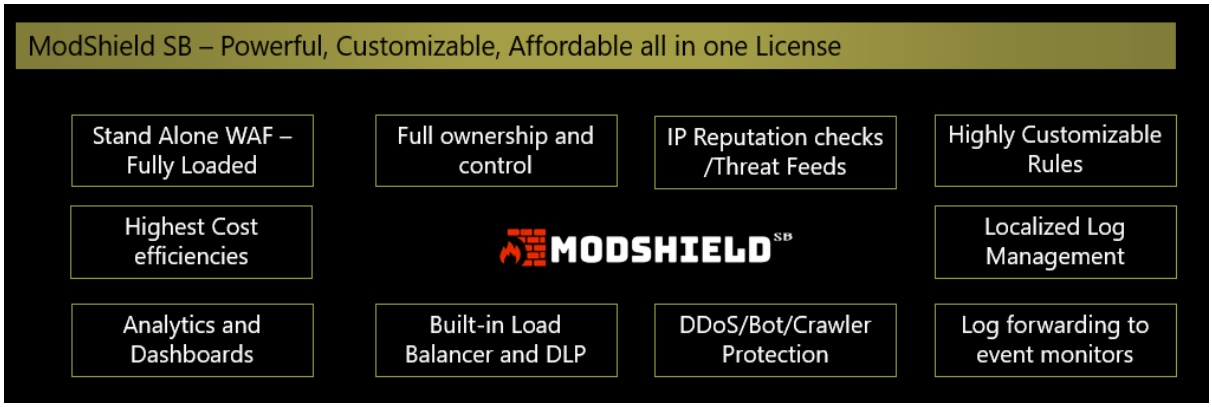
A web application firewall is a special type of application firewall that applies specifically to web applications. It is deployed in front of web applications and analyzes bi-directional web-based (HTTP) traffic - detecting and blocking anything malicious. The OWASP provides a broad technical definition for a WAF as "a security solution on the web application level which - from a technical point of view - does not depend on the application itself." According to the PCI DSS Information Supplement for requirement 6.6, a WAF is defined as "a security policy enforcement point positioned between a web application and the client endpoint. This functionality can be implemented in software or hardware, running in an appliance device, or in a typical server running a common operating system. It may be a stand-alone device or integrated into other network components." In other words, a WAF can be a virtual or physical appliance that prevents vulnerabilities in web applications from being exploited by outside threats. These vulnerabilities may be because the application itself is a legacy type or it was insufficiently coded by design. The WAF addresses these code shortcomings by special configurations of rule-sets, also known as policies.

WAFs are not an ultimate security solution, rather they are meant to be used in conjunction with other network perimeter security solutions such as network firewalls and intrusion prevention systems to provide a holistic defense strategy.

What is Modshield SB?



- Modshield SB is a web Application Firewall that is powerful and enterprise grade yet affordable and easy to implement
- Modshield SB is custom built using Modsecurity (the most trusted firewall by security engineers) and OWASP CRS (providing adequate coverage to application threats), adding analytics and intuitive configuration elements that are normally cumbersome
- Modshield SB is built for implementation on AWS, Alibaba cloud and as a Virtual machine
- StrongBox IT continuously update the custom rulesets and threat intelligence feeds thereby, eliminating the need for the business to ensure regular updates

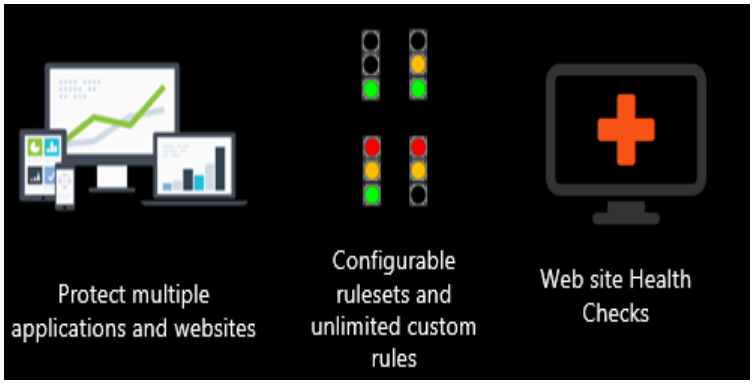


Modshield SB – Powerful at heart

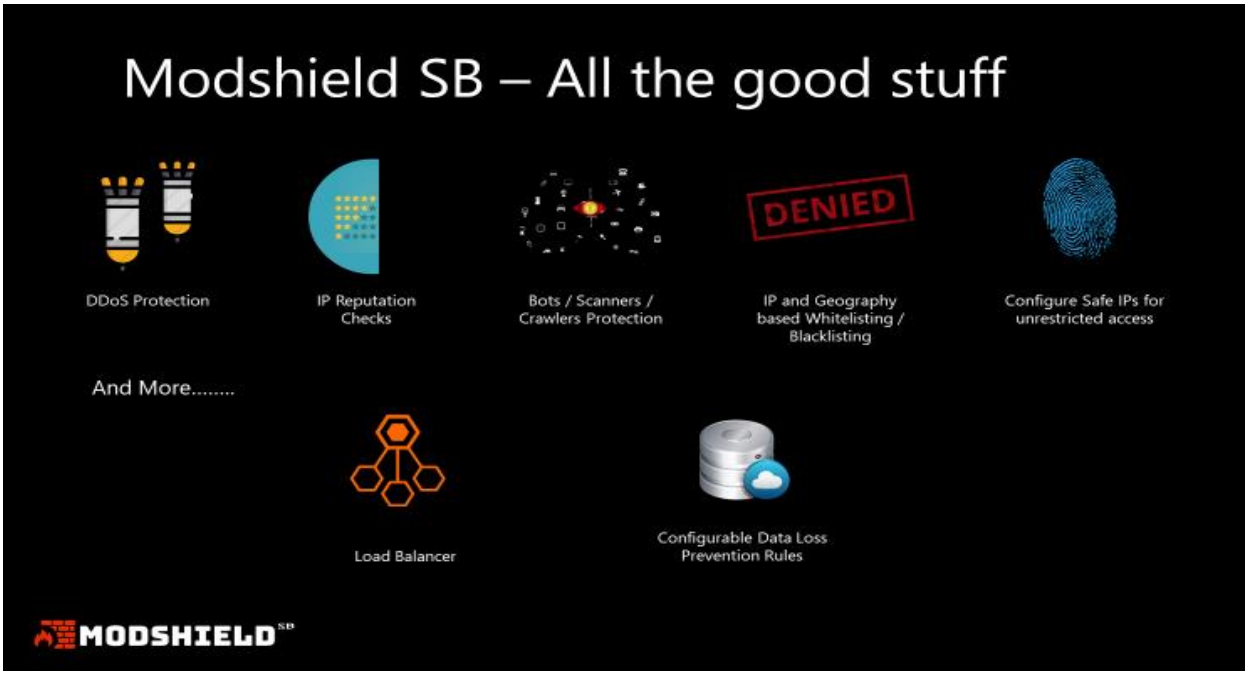
A customized implementation of Modsecurity and OWASP Core rule set to protect your web and mobile applications

- Straight through implementation – no technical experience required
- Available on AWS, Alibaba and as a Virtual Machine
- SSL Support – included

- Protect unlimited domains and applications
- Continuously updated rule sets – included
- Unlimited custom rules – included
- Health checks – included



Modshield SB – All the good stuff



Purpose of the document

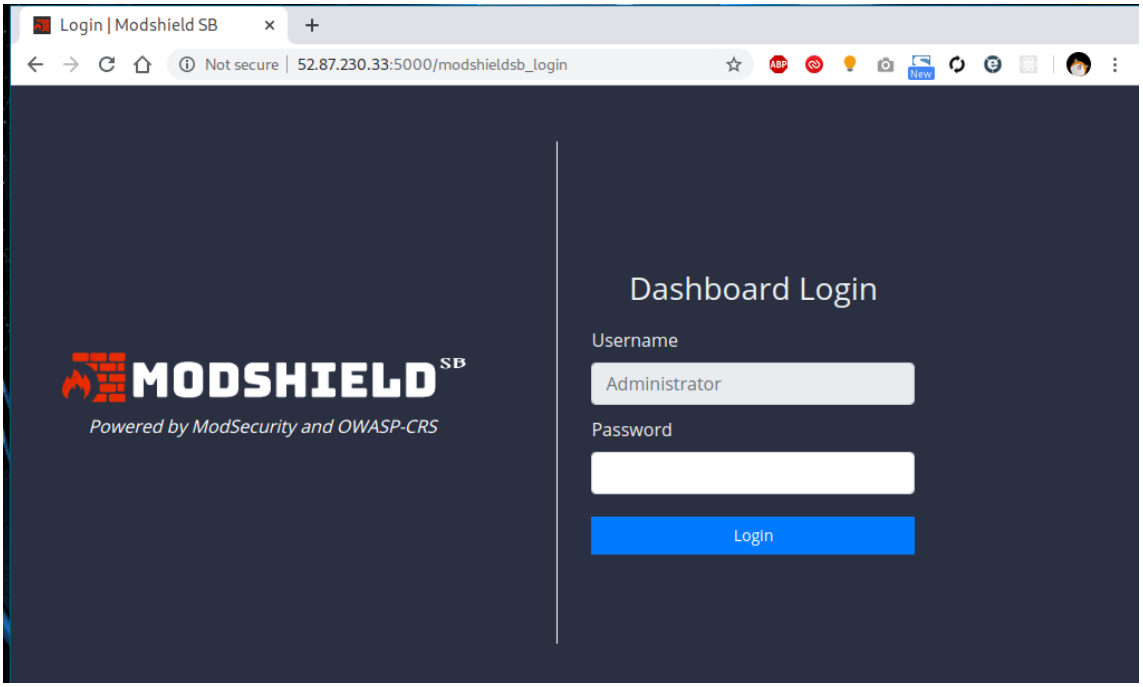
The purpose of this document is to help a Modshield user make use of the powerful and extremely useful features that Modshield provides. The document has been divided into sections addressing the basic setup and the advanced fine-tuning options that Modshield provides.

For additional help, please write to ms_support@strongboxit.com

Installing Modshield SB VM Image

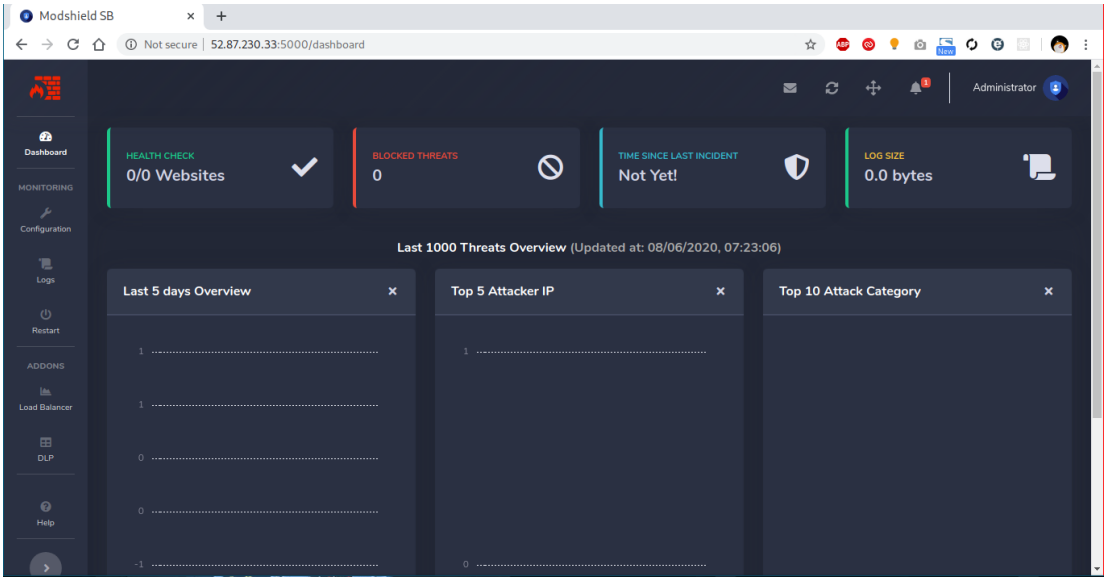
Step No: 1 Download the VM image from the FTP link provided and upload it to a VM manager. Please allocate a 4 core, 16 GB RAM instance with a minimum of 100 GB of free space. Please ensure that the instance has an active internet connection. Assign a static IP address to this instance if the VM will be accessed externally.

Step No2: Visit **http://<Public IP>:5000/modshieldsb_login** to access the administrative panel



Enter the provided password in the password field to login.

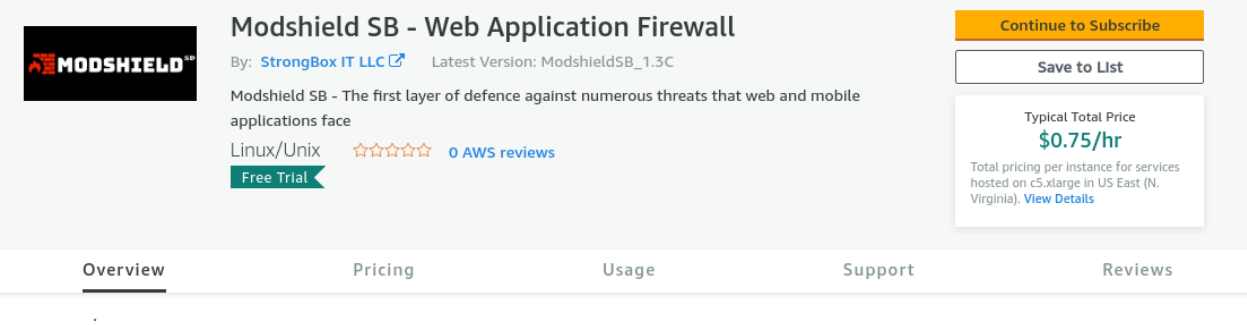
You should now be greeted with the empty dashboard page as follows



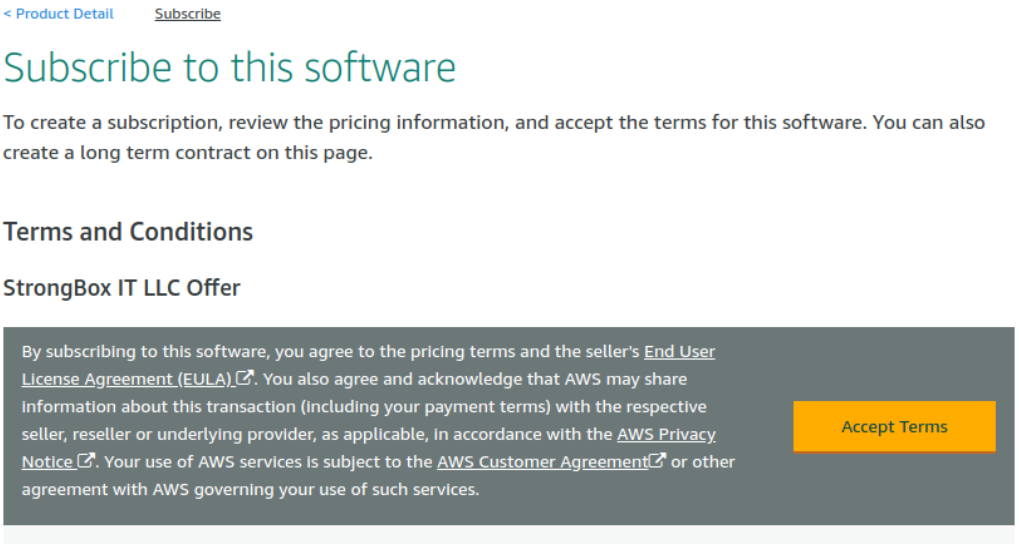
You will be prompted to change the password on login. Please proceed to the section: Adding a Domain to Modshield SB to continue configuring Modshield SB for the applications that you desire to protect

Installing Modshield SB from the AWS Marketplace

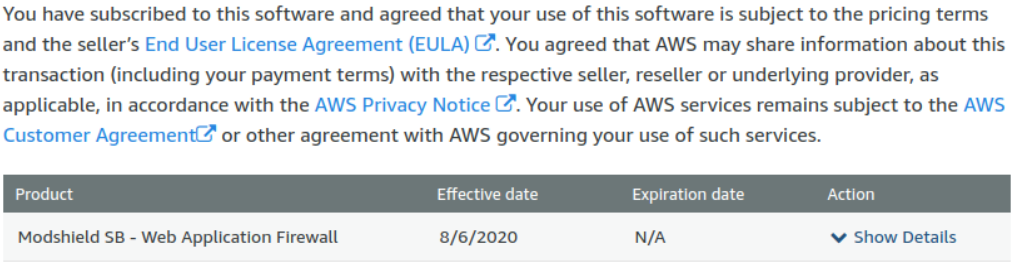
Step No: 1 Visit the marketplace page of the version that better suits your needs (Cloud / BYOL). Click on "**Continue to Subscribe**" button



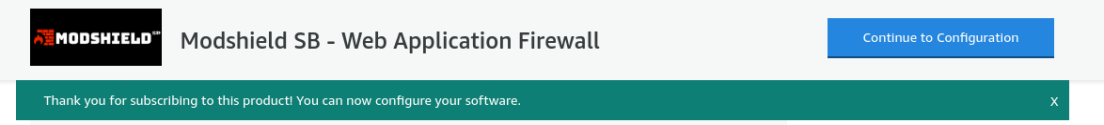
Step No: 2 Read and confirm that you accept the **End User Licence Agreement** (EULA)



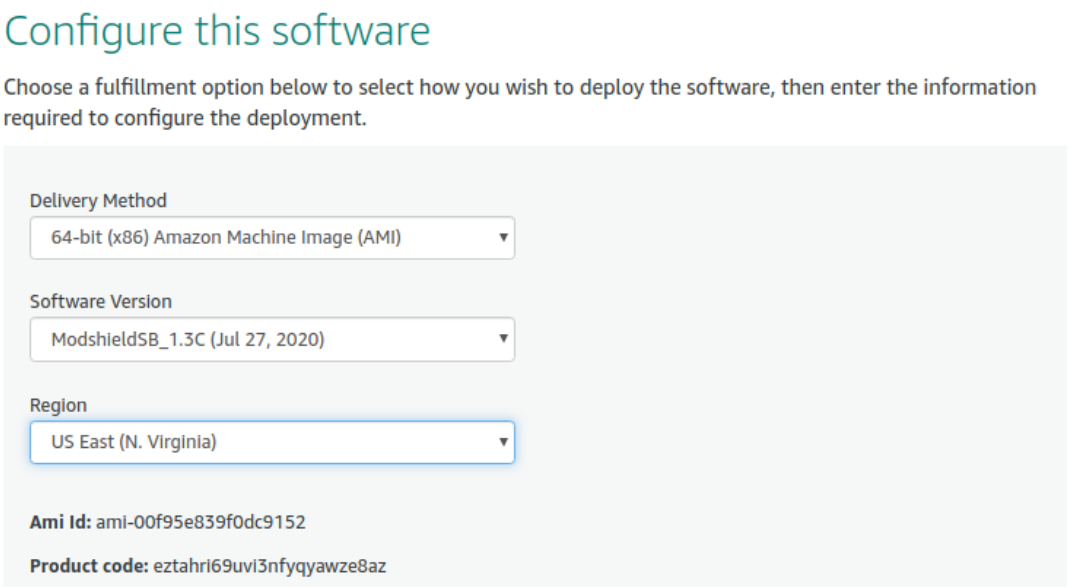
Step No: 3 You should see the status as **"Pending"** for a while when AWS processes your request, which should eventually change to the date when you accepted the EULA



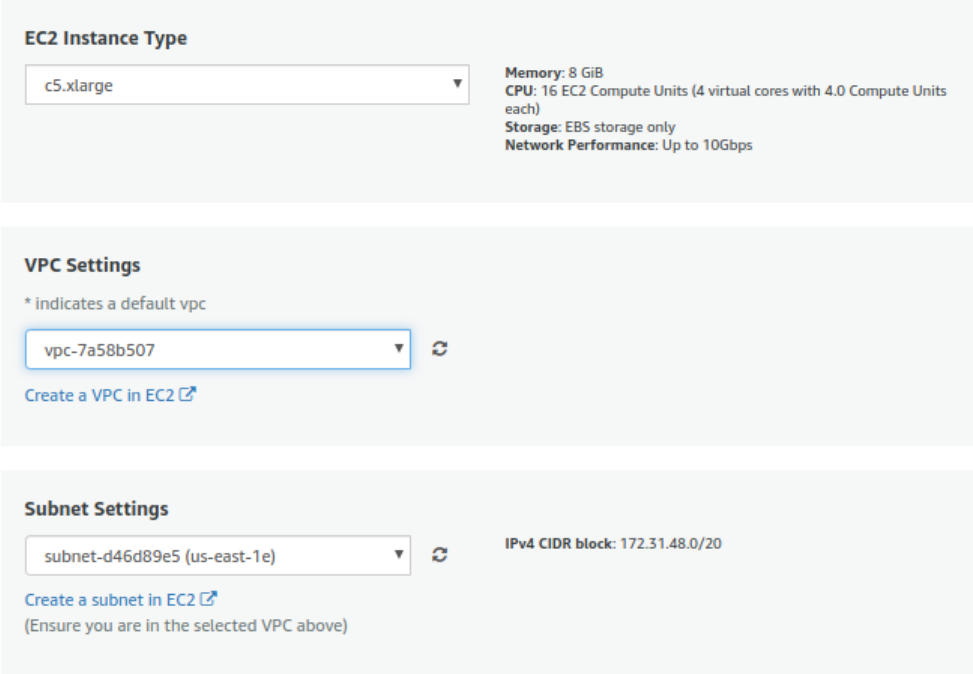
Step No: 4 Click on **"Continue to Configuration"** button on top right to configure your instance



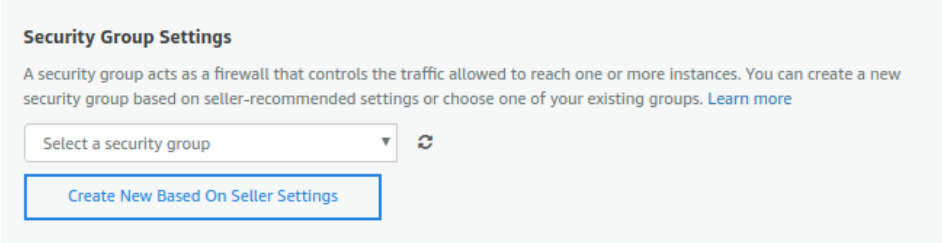
Step No: 5 Confirm the Modshield SB version and Region that you want the instance to be deployed, and click the **"Continue to Launch"** button



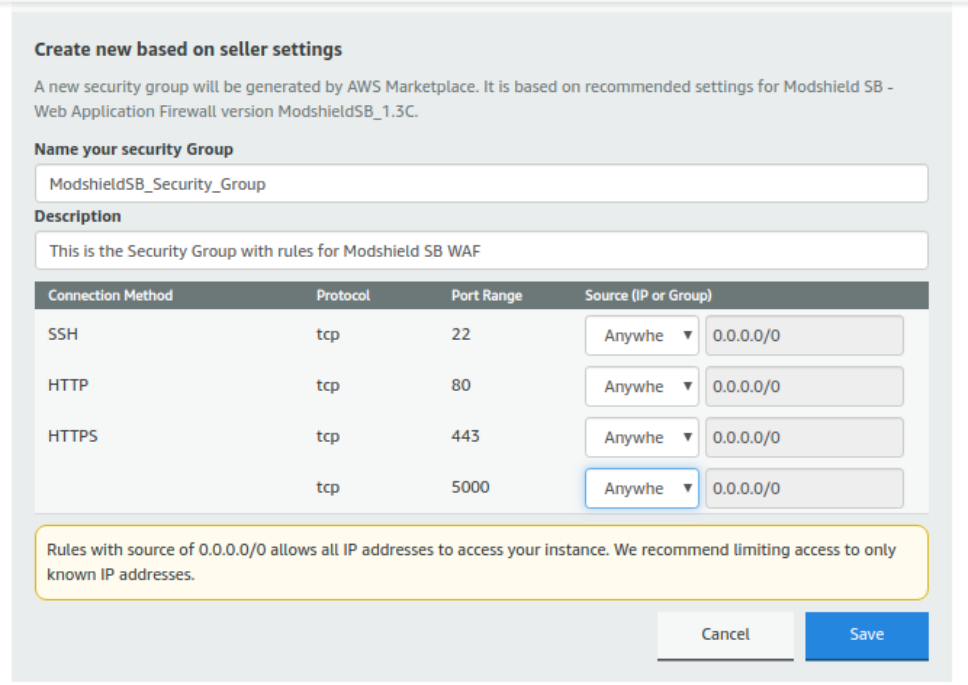
Step No: 5 Confirm the Instance Type, VPC and subnet settings in the following page as per your needs, or you can use the recommended defaults



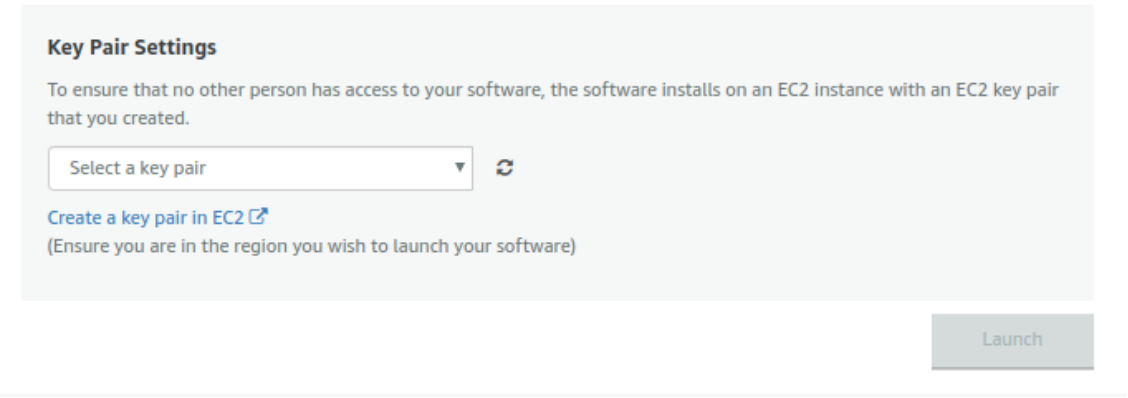
Step No: 6 Since Modshield SB requires ports 22,80,443,5000 open for access to administrative panel and normal operations, you can either click on **"Create New Based on Seller Settings"** to pre-populate the security group, or configure a new security group as per your requirements



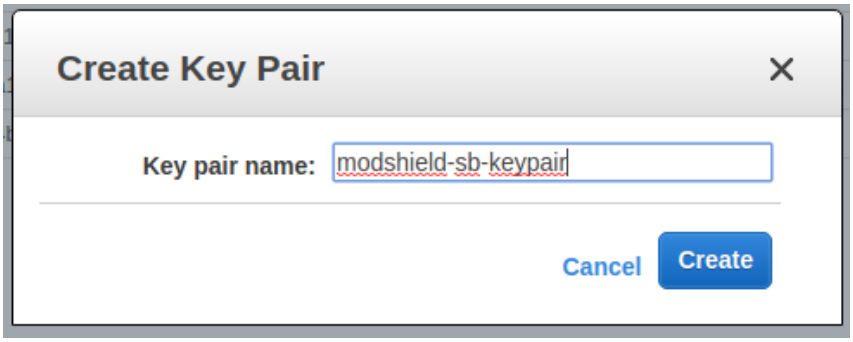
Step No: 7 Enter name and description for the new security group, and click on **"Save"** Button. You can also restrict access to the administrative panel by allowing access only from a particular IP or range of IPs by modifying the Source IP fields at this step



Step No: 8 Create keypair for the new instance by selecting the **"Create new keypair in EC2"** link which takes you to the Keypair section in EC2

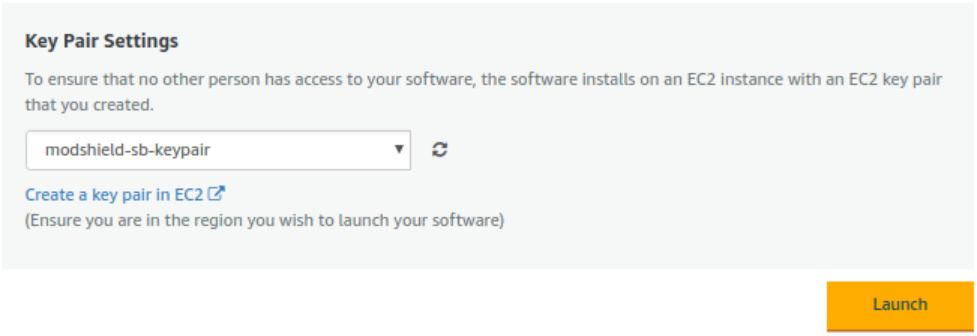


Step No: 9 Click on **"Create new keypair"** and give suitable name

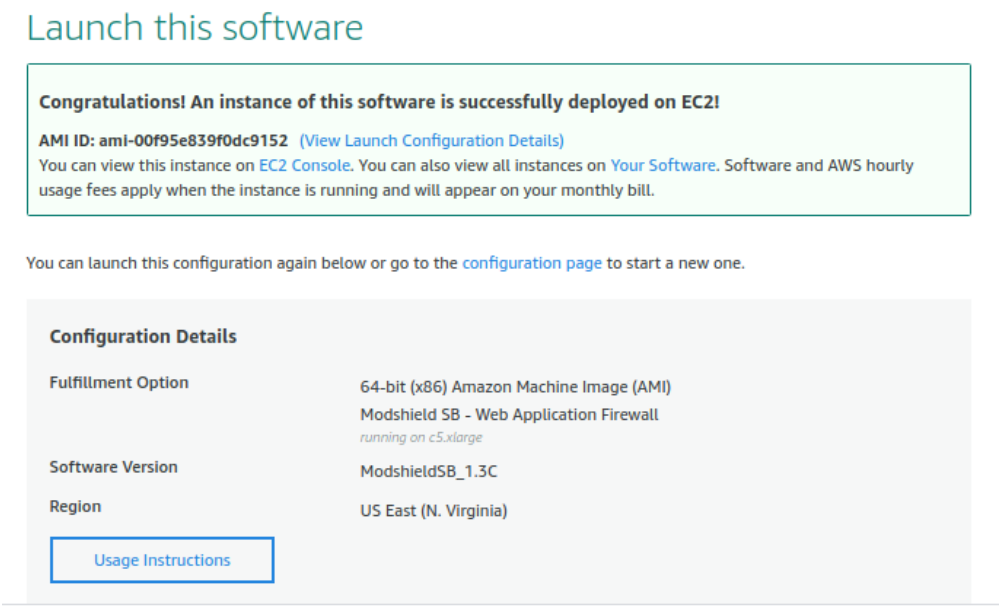


Step No: 10 Once you click on **"Create"** button in the previous step, save the generated keypair file in PEM format to a safe and secure location

Click the button with the refresh symbol, and select the newly generated keypair from the list. Click on **"Launch"** button to start your instance



Your instance should now be deployed to your EC2 console

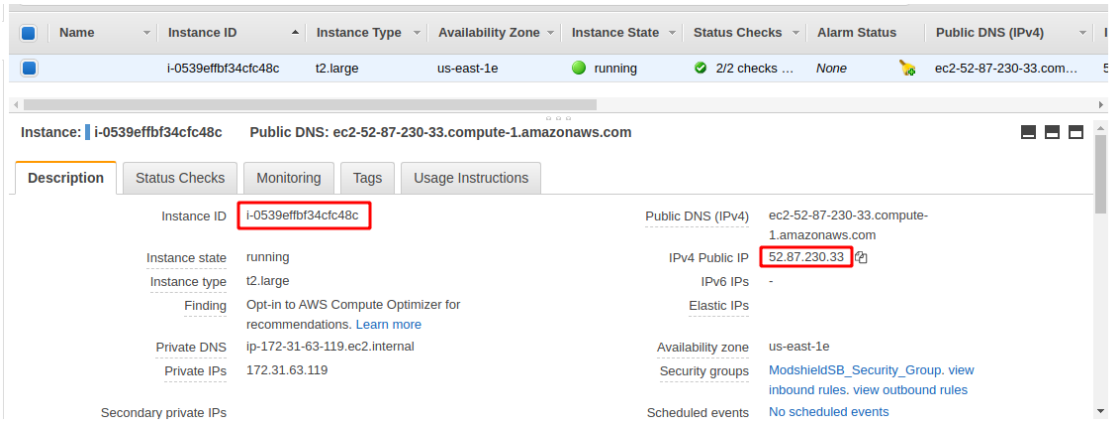


In the next section, we will check on accessing the dashboard, and configuring various domains and related settings

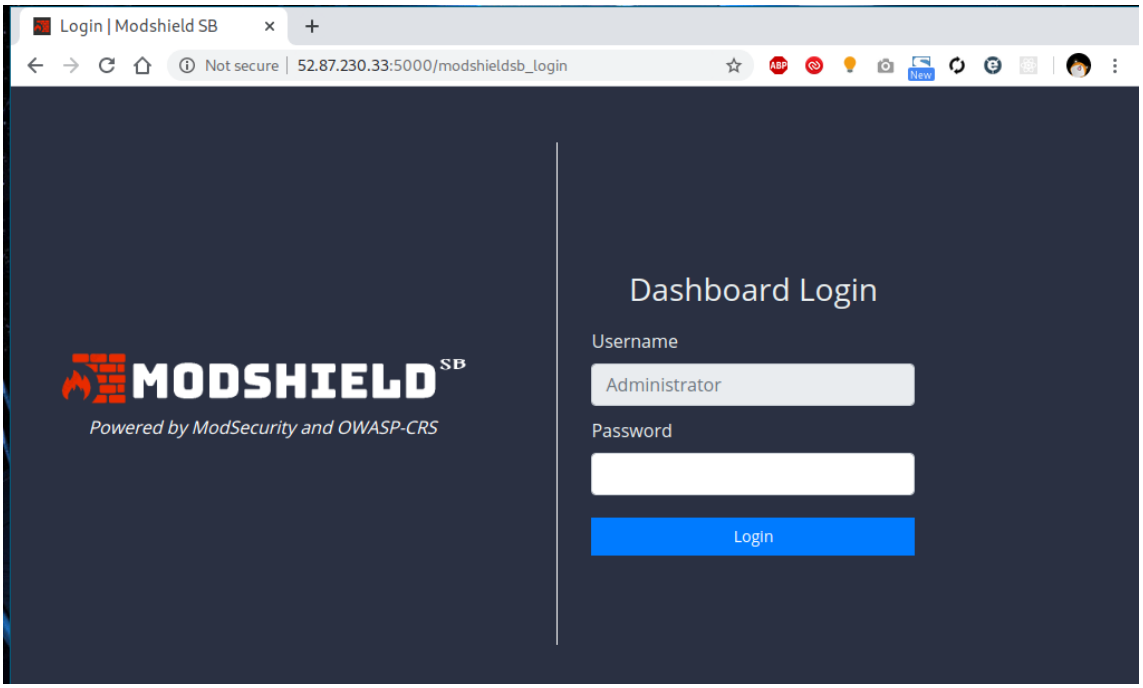
Accessing dashboard

Click on the **"EC2 Console"** link in previous step to take you directly to the page where your instance is running

Note the **Instance ID** (which will be the initial password), and **Public IP** of the WAF instance

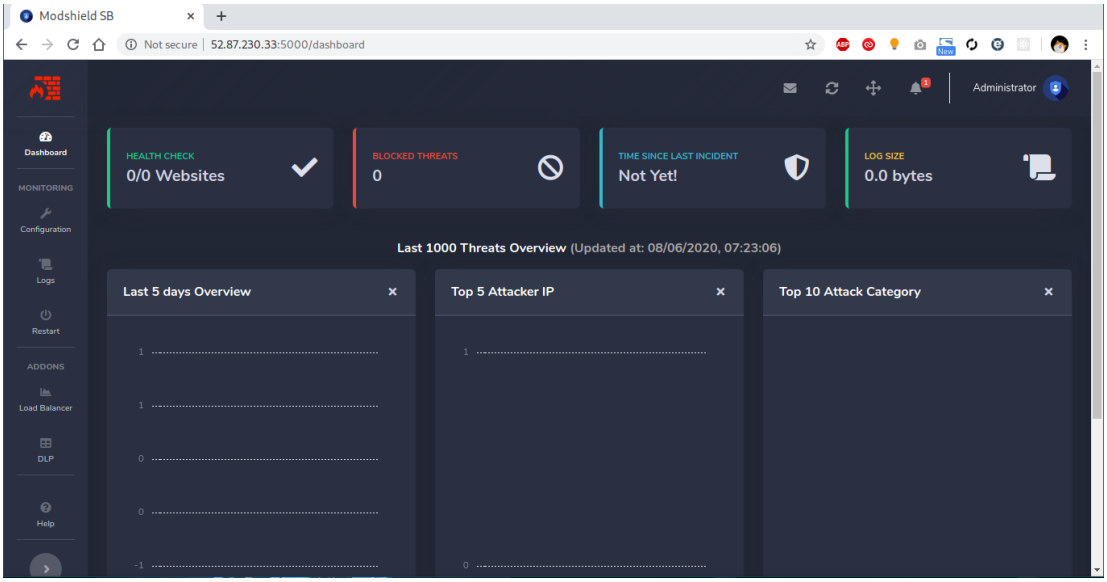


Visit **http://<Public IP>:5000/modshieldsb_login** to access the administrative panel



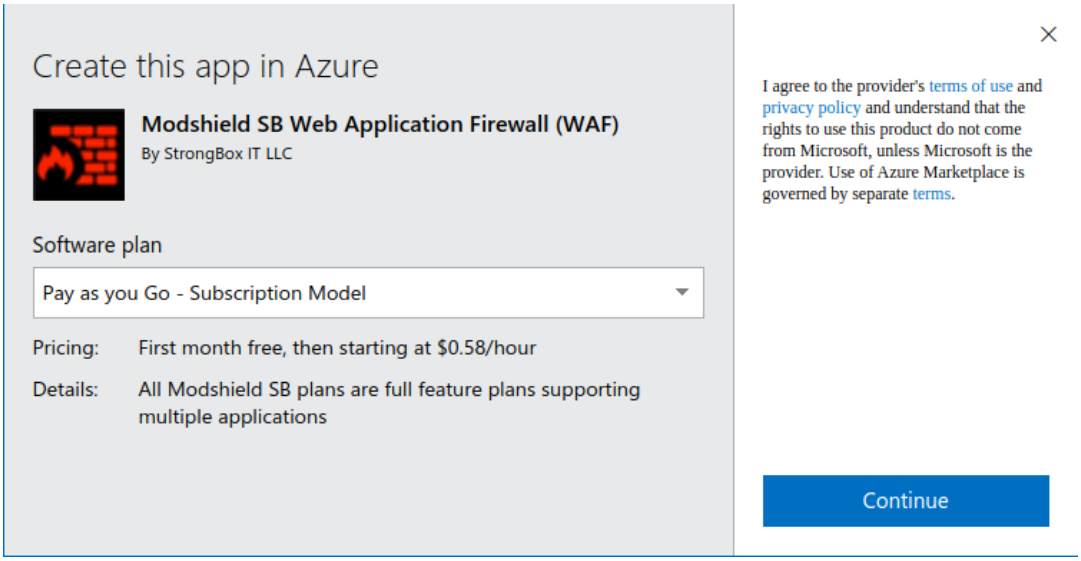
Enter your **instance ID** in the password field to login

You should now be greeted with the empty dashboard page as follows

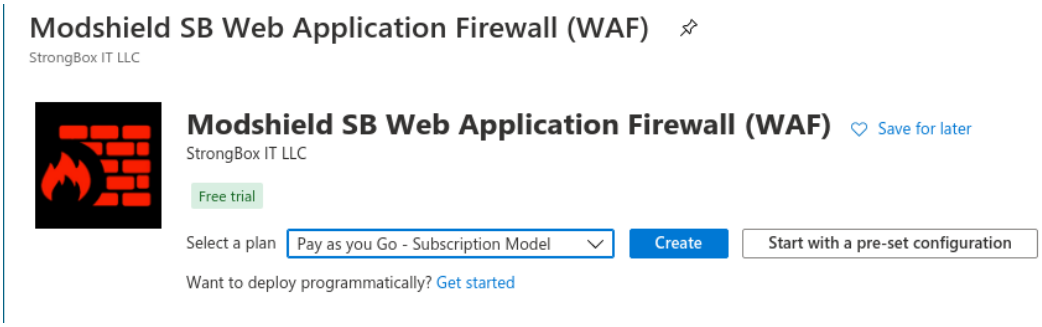

Modshield SB
Not secure | 52.87.230.33:5000/dashboard
Administrator
Dashboard
MONITORING
Configuration
Logs
Restart
ADDONS
Load Balancer
DLP
Help
HEALTH CHECK
0/0 Websites
BLOCKED THREATS
0
TIME SINCE LAST INCIDENT
Not Yet!
LOG SIZE
0.0 bytes
Last 1000 Threats Overview (Updated at: 08/06/2020, 07:23:06)
Last 5 days Overview
Top 5 Attacker IP
Top 10 Attack Category

Installing Modshield SB from the Azure Marketplace

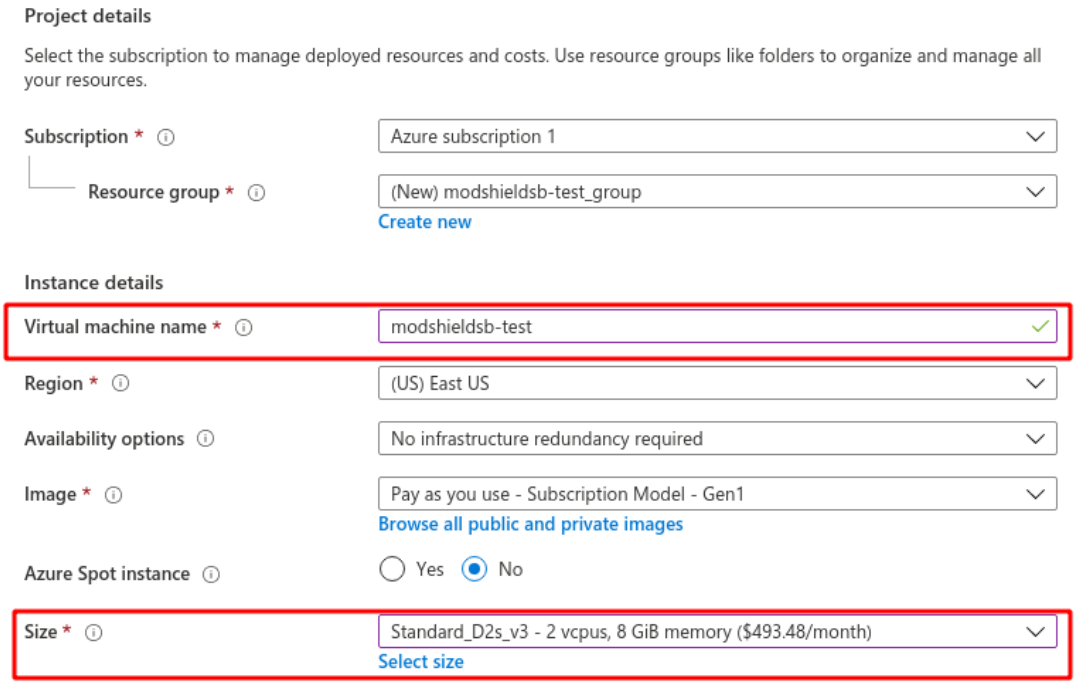
Step 1: Select your preferred plan (either Cloud or BYOL) from the provided dropdown menu, and click **Continue** button



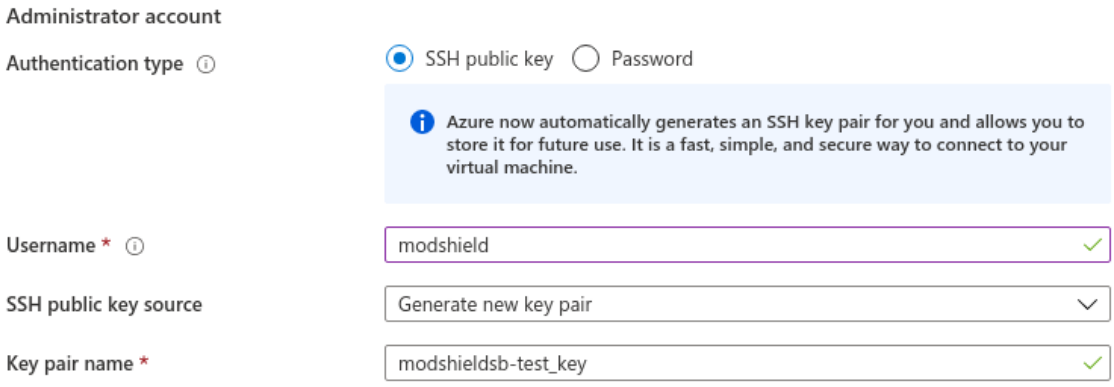
Step 2: Click on **Create** button to configure various deployment settings



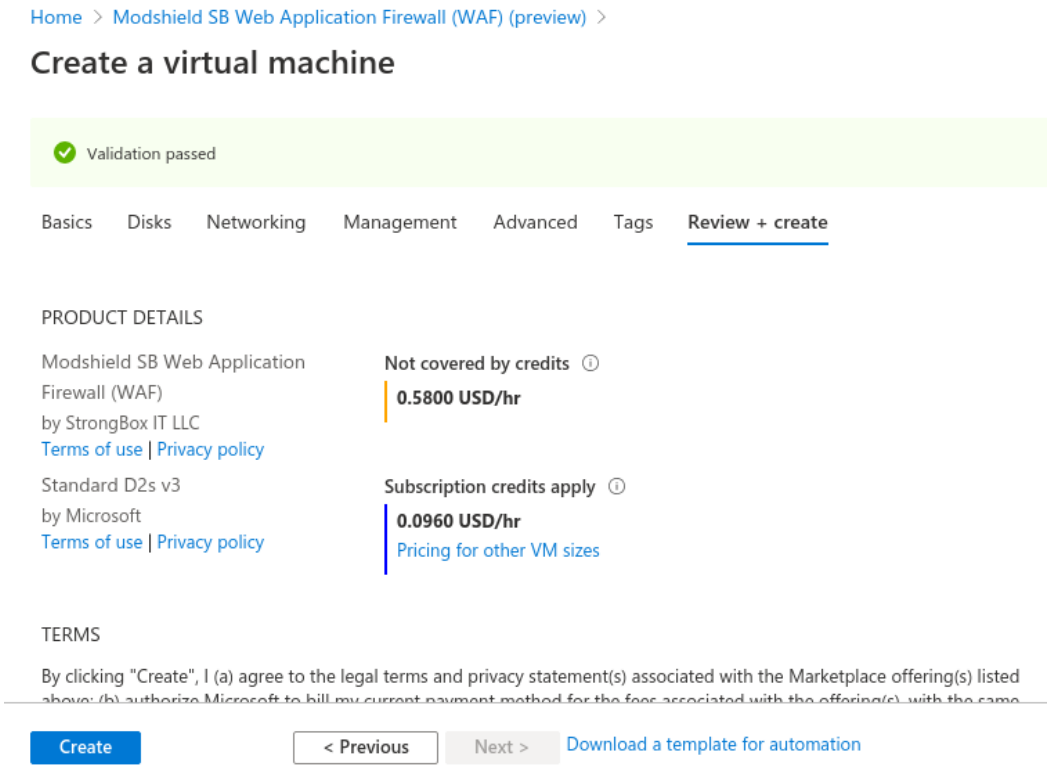
Step 3: Provide **name** for your new instance and change **size** if required from the available list



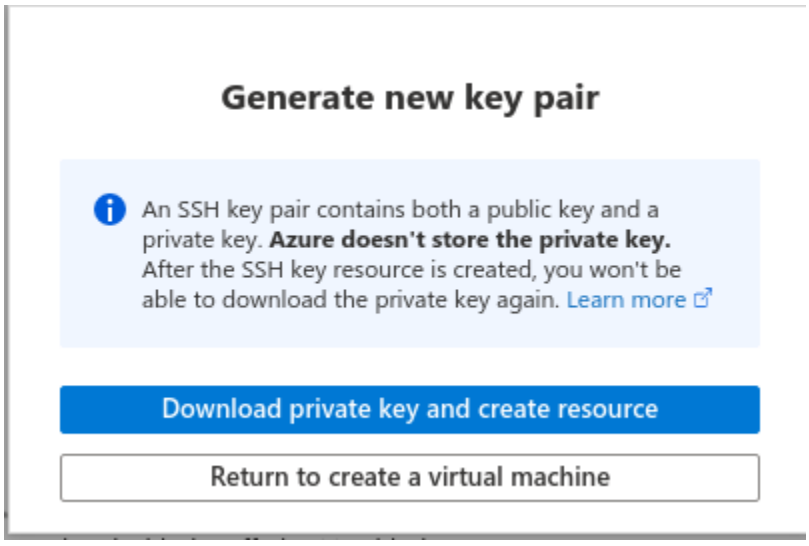
Step 4: Configure your login username and authentication method in the next step. NOTE: You can also opt to use the default **modshield** username to simplify user management.



Step 5: Click on **Review+Create** button to review the final deployment template and click on **Create** button.



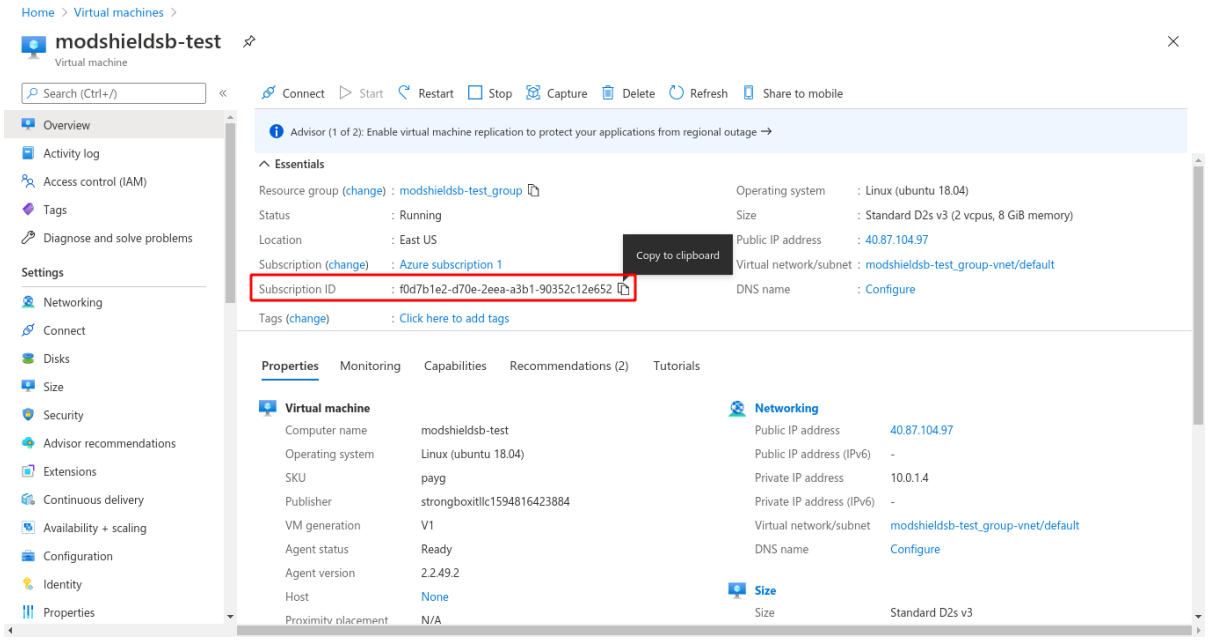
Step 6: Save the SSH private key when prompted and click Download private key and create resource button to deploy your instance



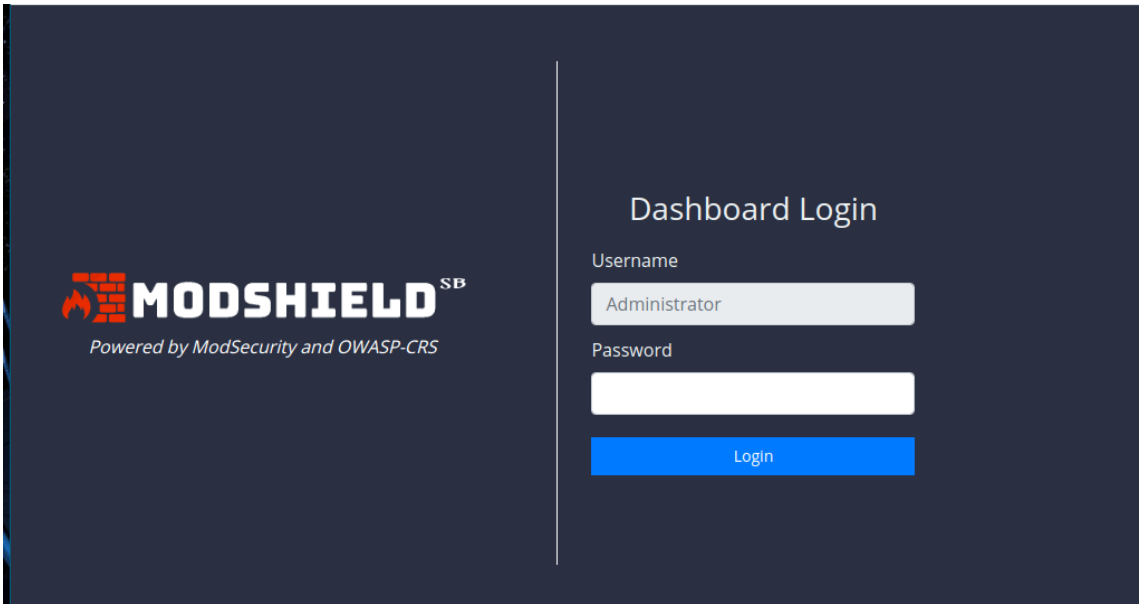
In the next section, we will check on accessing the dashboard, and configuring various domains and related settings

Accessing dashboard

Once your new instance is deployed, copy the **Subscription ID**, which would be default password for your Modshield SB instance

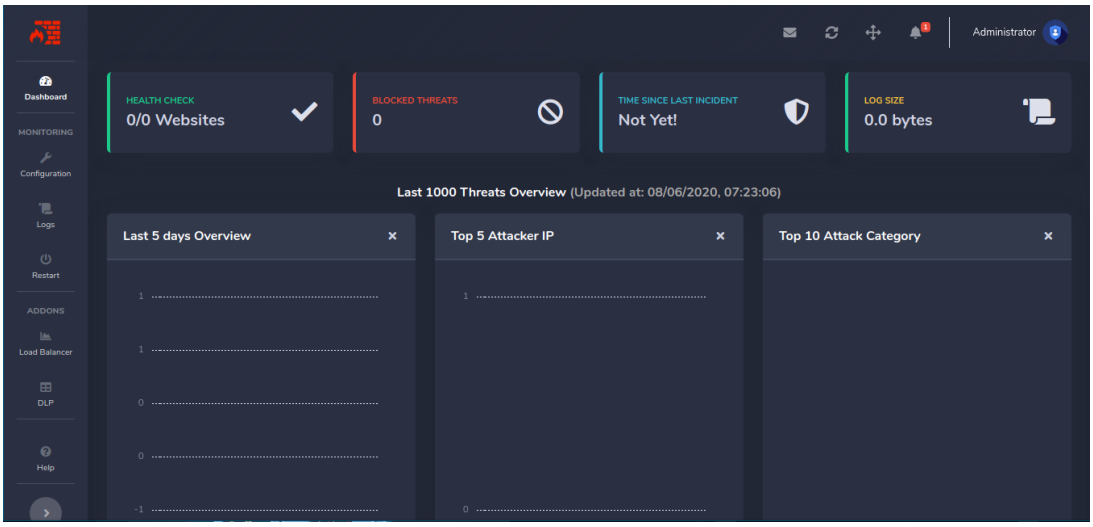


Visit **http://<Public IP>:5000/modshieldsb_login** to access the administrative panel



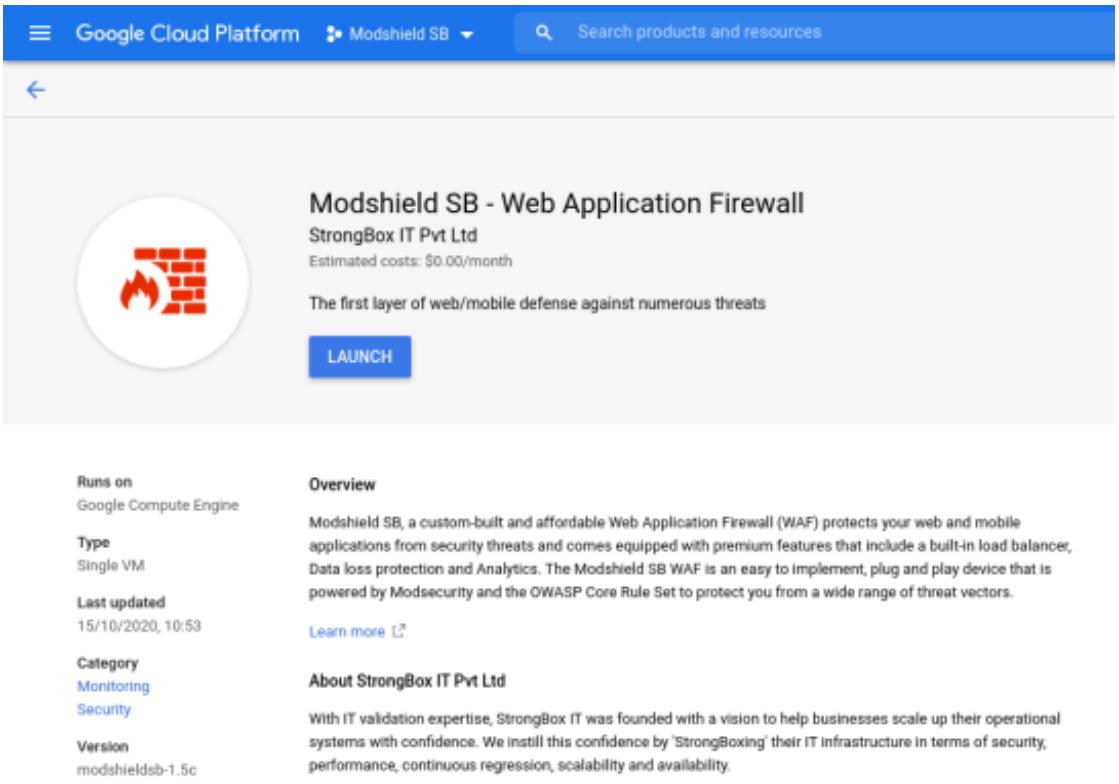
Enter your **Azure Subscription ID** in the password field to login

You should now be greeted with the empty dashboard page as follows

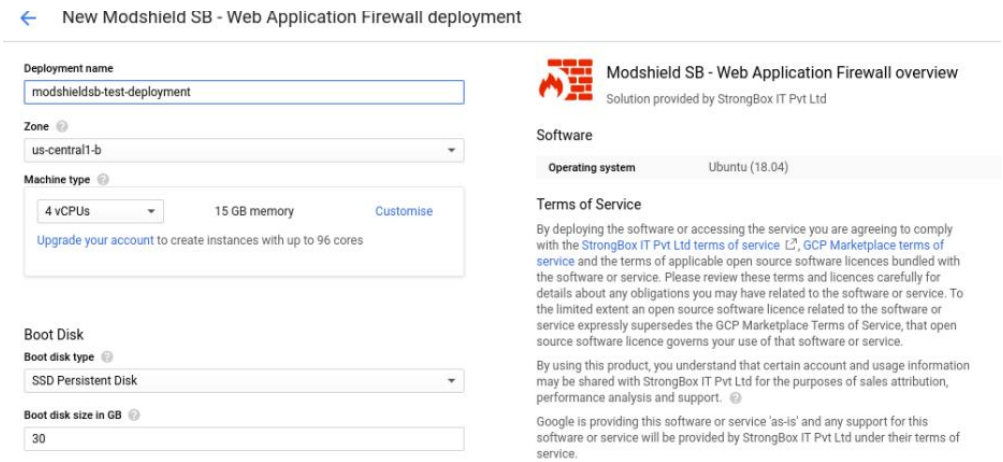


Installing Modshield SB from the GCP Marketplace

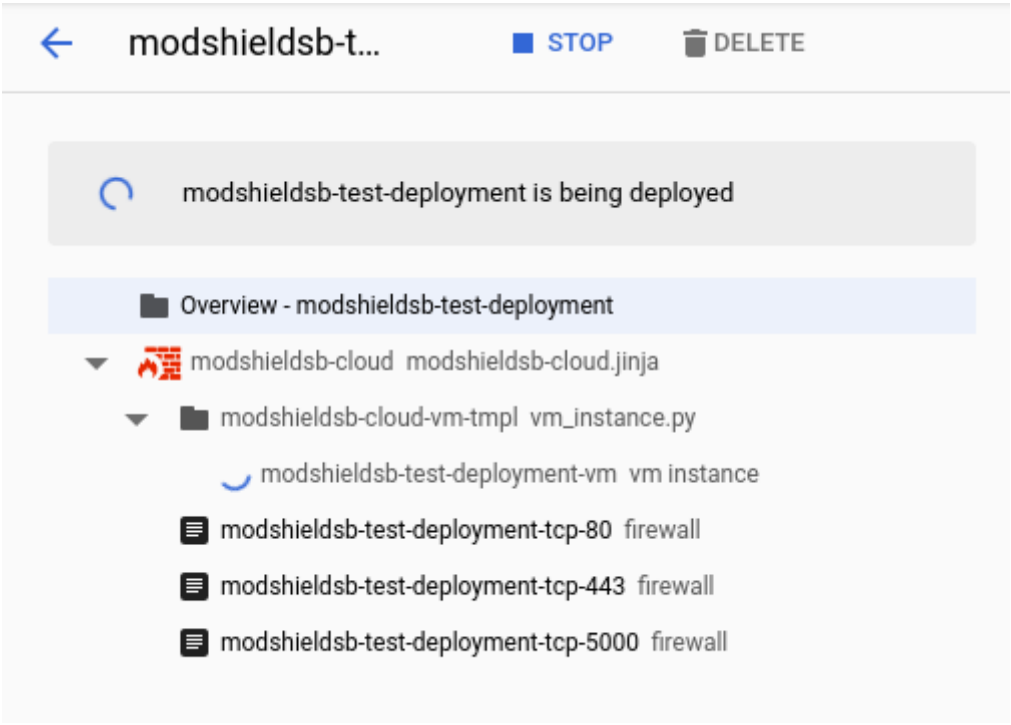
Step 1: Open the GCP Marketplace listing page that suits your licensing model (Cloud / BYOL), and click on the **Launch** button.



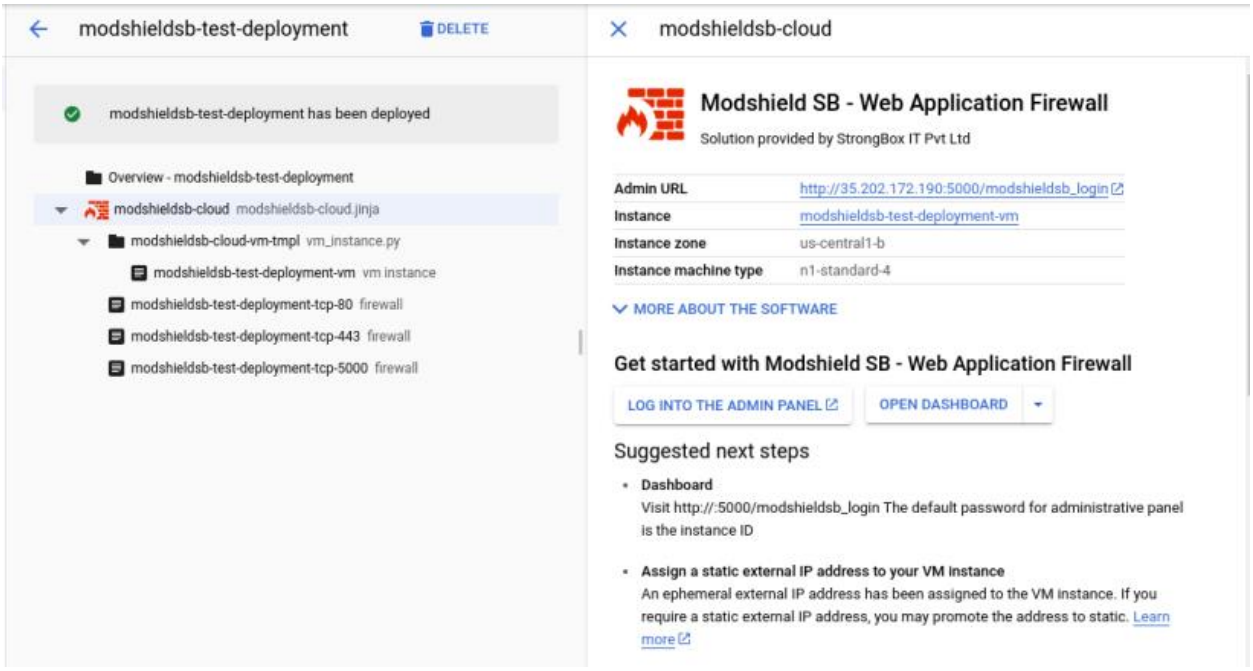
Step 2: Provide a suitable **instance name** for your new deployment. Change the **Deployment Zone** and **Machine Type** if required, while it's recommended to use the deployment template defaults. **Disk Size** can be increased if logs are to be rotated less frequently or in systems requiring high traffic



Step 3: Click on the **Deploy** button once all the settings are finalized

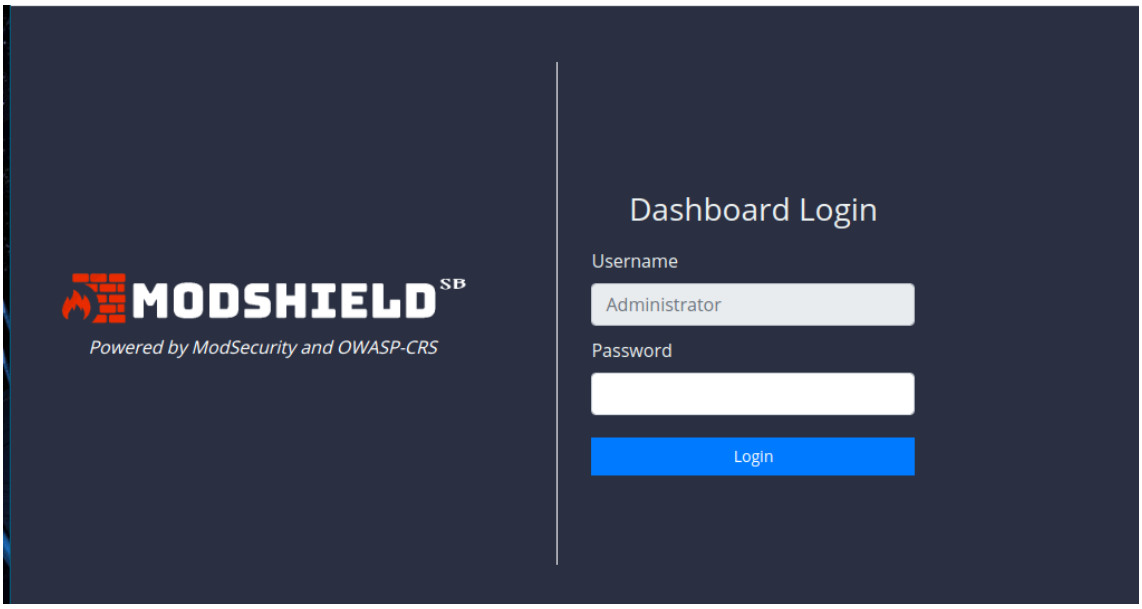


Step 4: Select the deployed package overview link in the left pane and open the **Admin Panel URL** from the right pane to launch the administrative console.



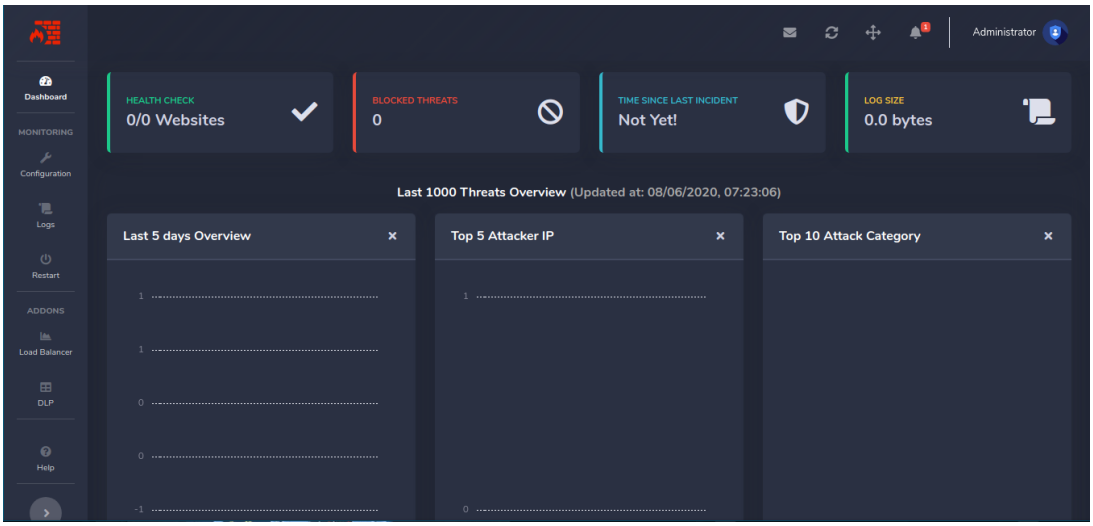
Accessing dashboard

Once your new instance is deployed, copy the **Instance ID**, which would be default password for your Modshield SB instance



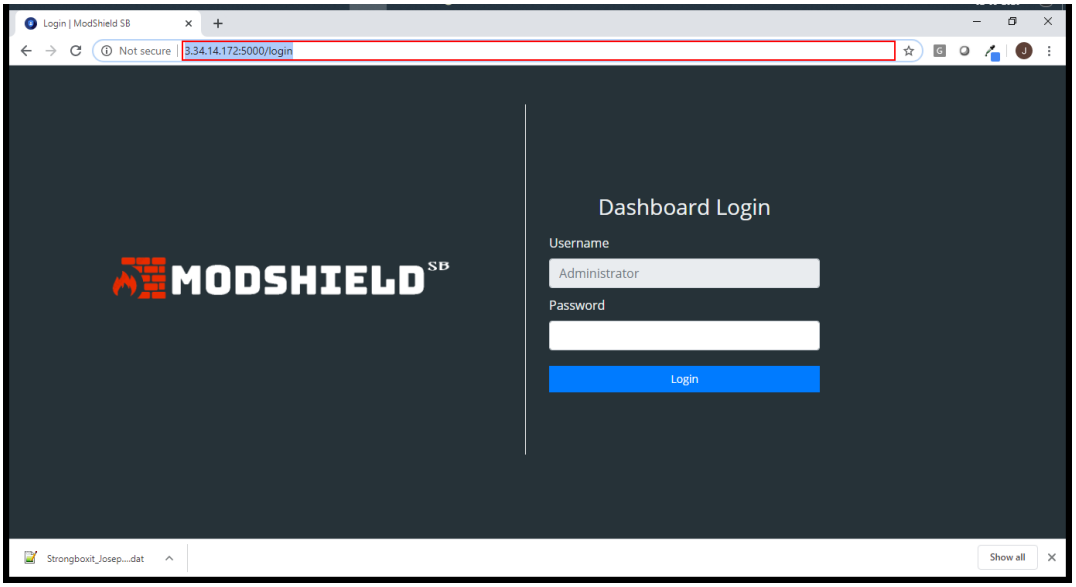
Enter your **GCP Instance ID** in the password field to login

You should now be greeted with the empty dashboard page as follows

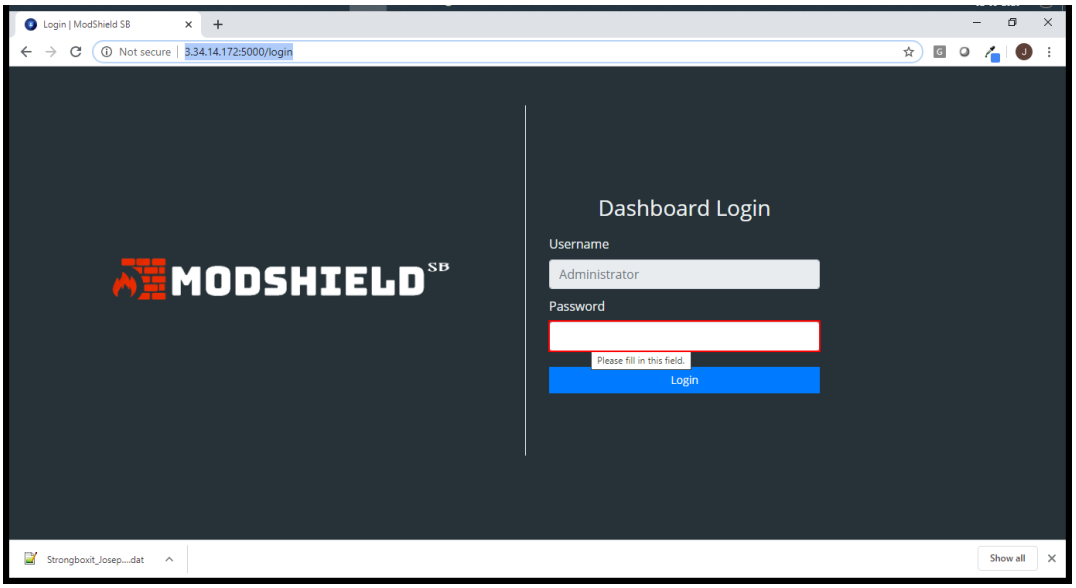


Setting up a Domain in Modshield SB

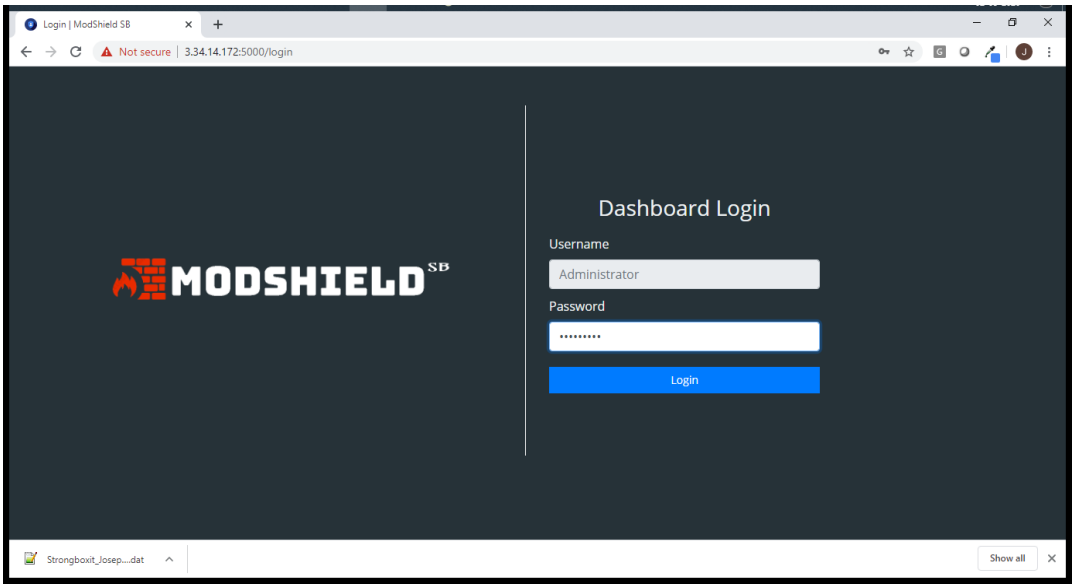
Step No: 1 To add a domain, login to your Modshield instance.



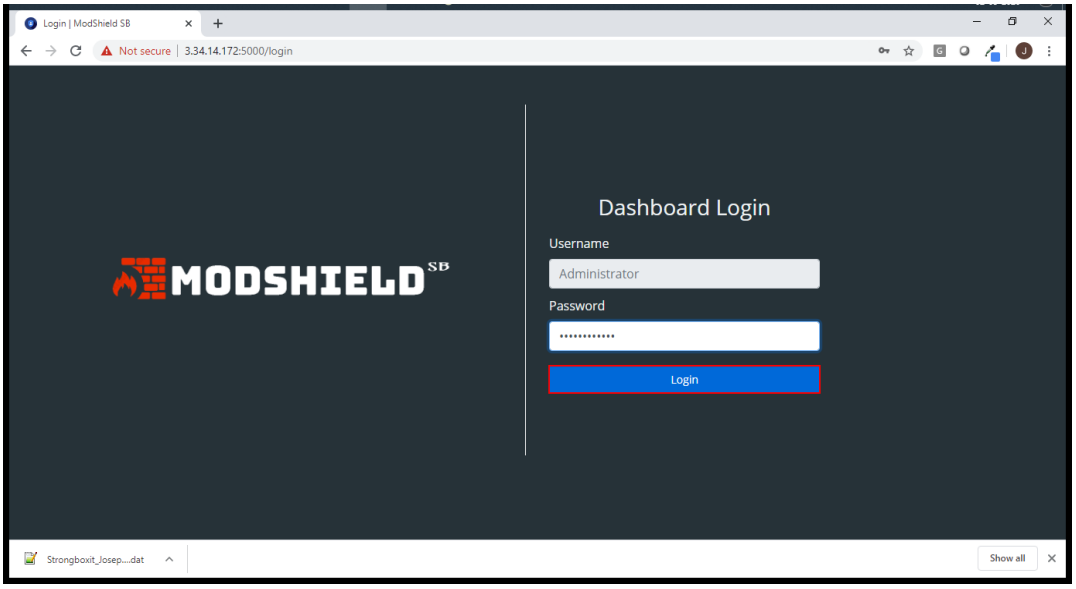
Step No: 2 Based on your implementation, this could be a VM or a cloud instance



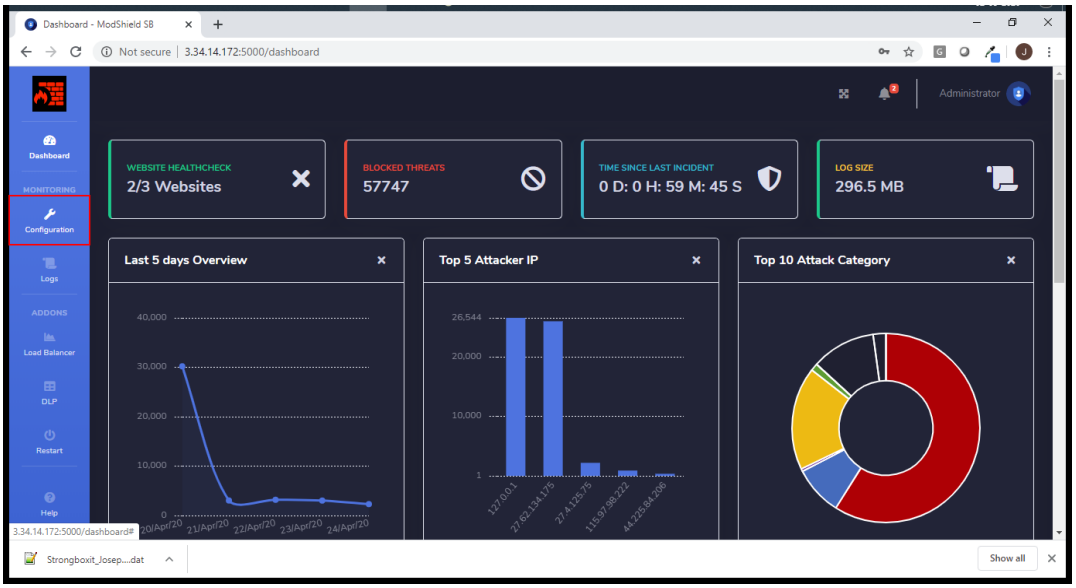
Step No: 3 Before you begin, configure the DNS for your domain to point to the Modshield SB IP address



Step No: 4 Enter your Modshield password and login



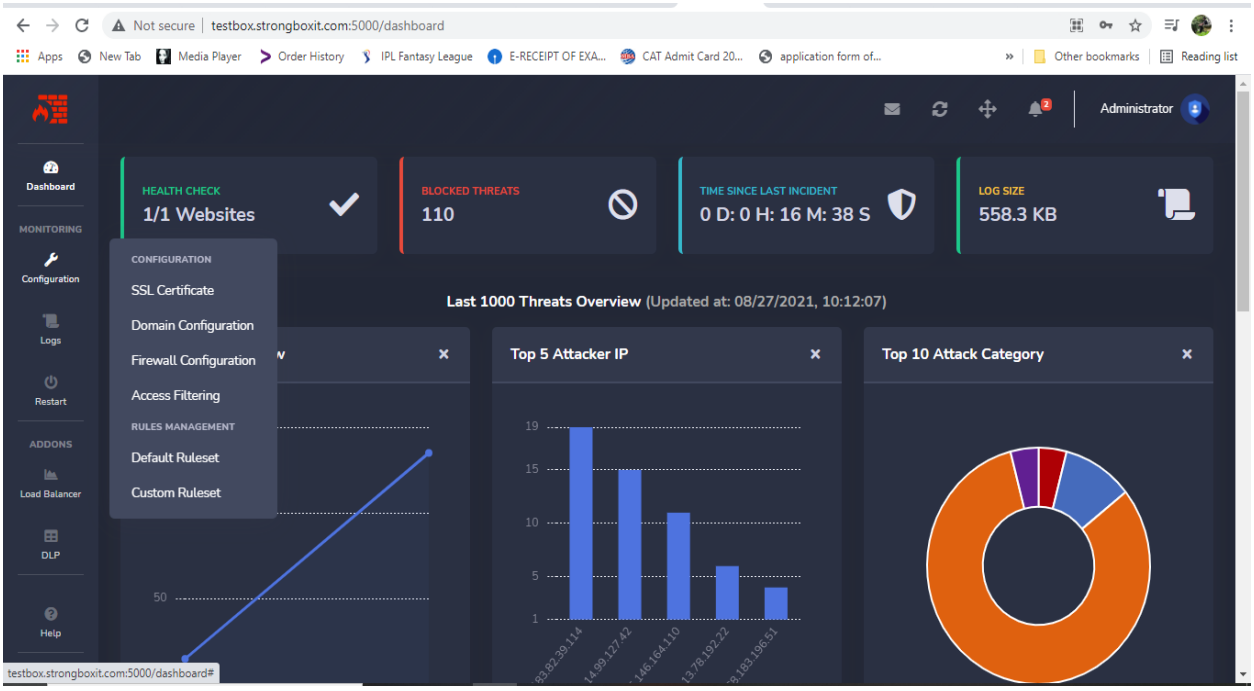
Step No: 5 This dashboard will be blank if you are configuring your first website or application



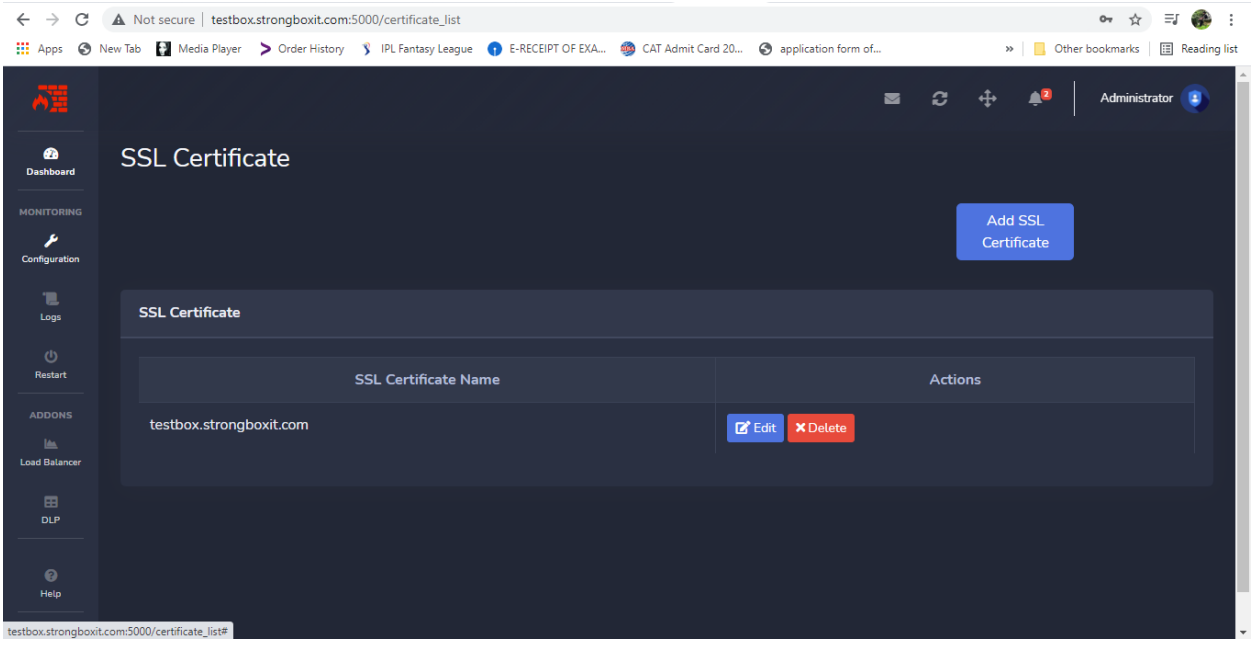
If your domain has a SSL Certificate, you will be required to complete the addition of SSL certificates first. This will later be associated to the domains that you configure in Modshield SB. If you are adding a HTTP application, you can skip the next section and continue from Adding a Domain to Modshield SB

Adding SSL certificate to Modshield SB

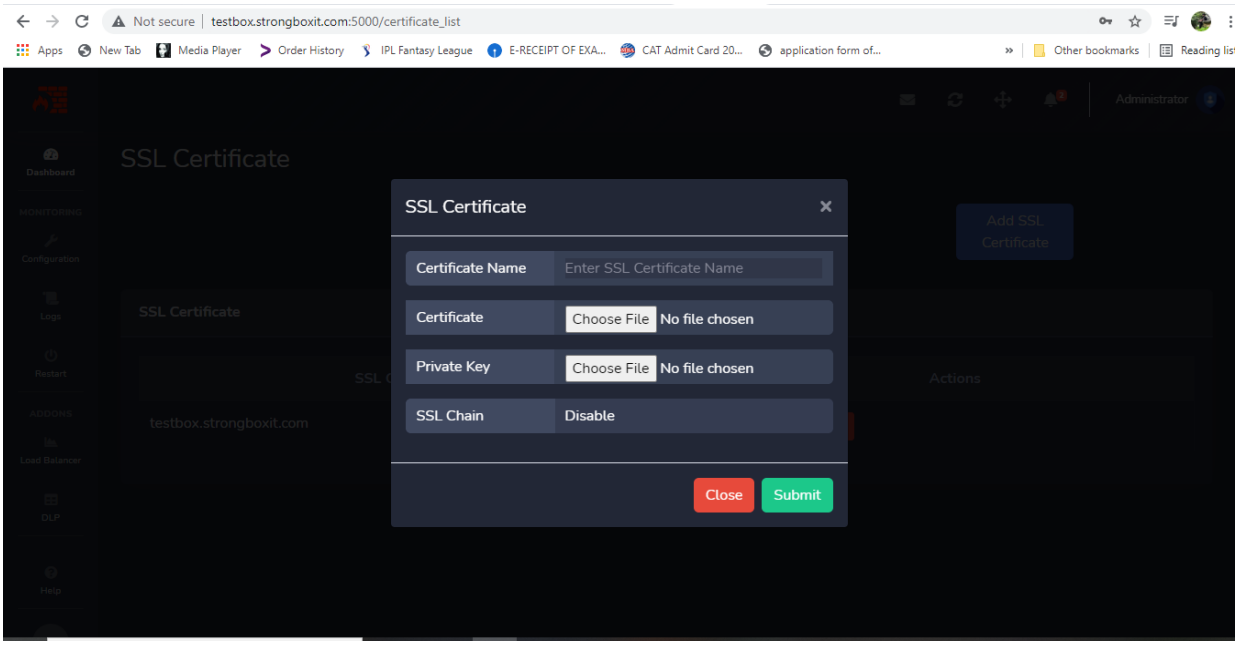
Step no 1: To add SSL certificate click on configuration ->SSL certificate



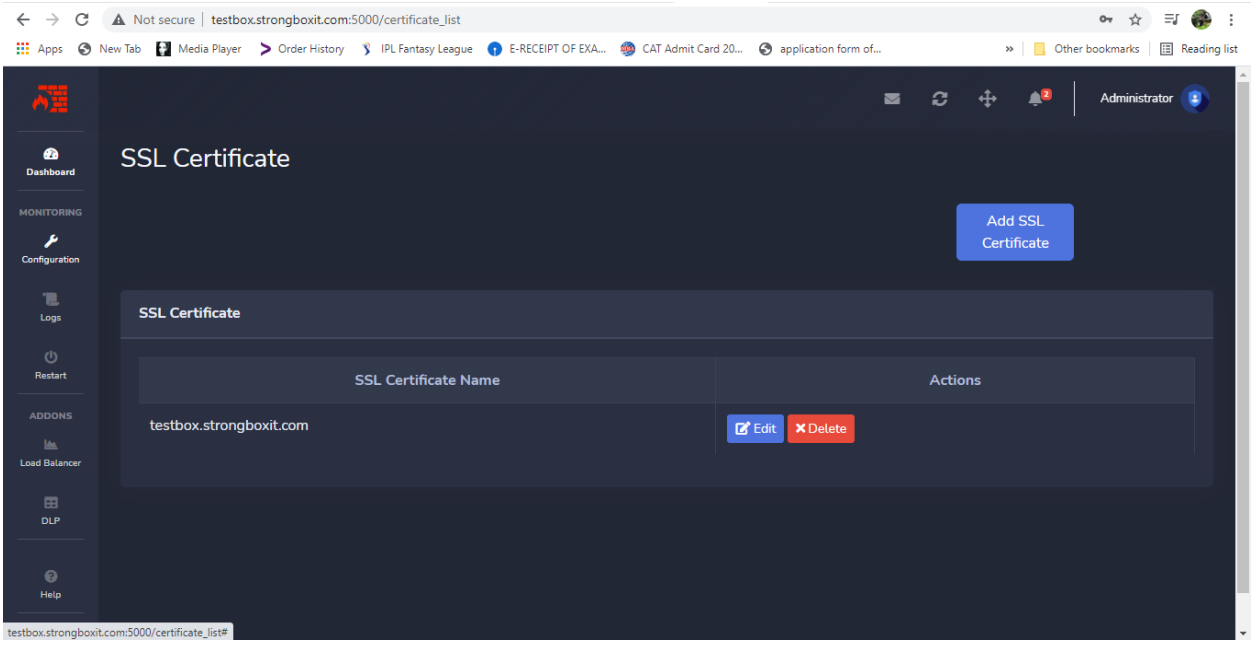
Step 2: Click on Add SSL certificate icon to add your certificate. You can also view, edit and delete your existing certificates.



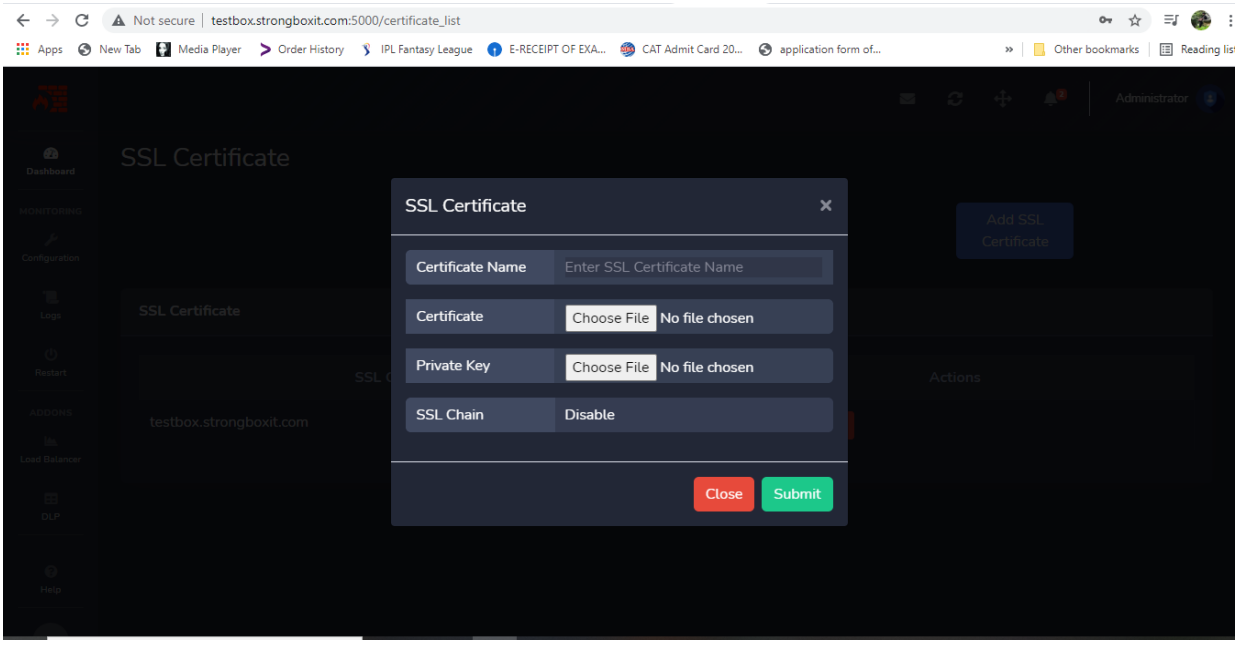
Step 3: SSL Certificate dialog box appears. Click on choose file option in certificate column and upload your certificate. Click on submit.



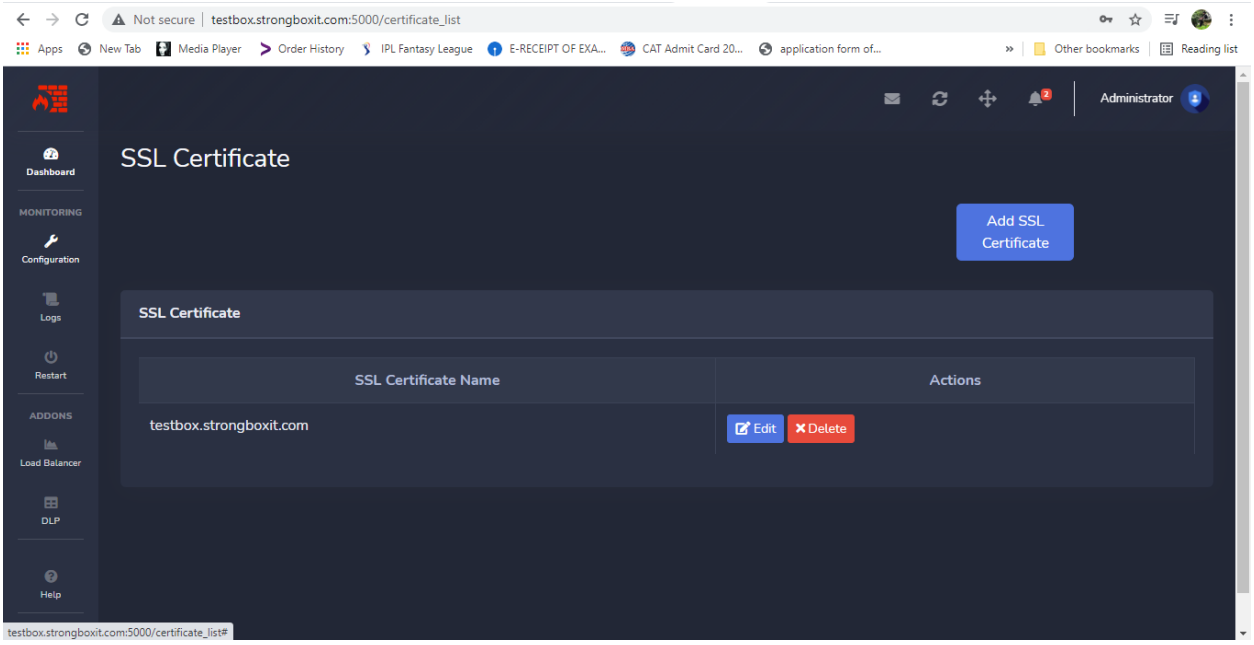
Step 4: To edit your certificate click on edit icon.



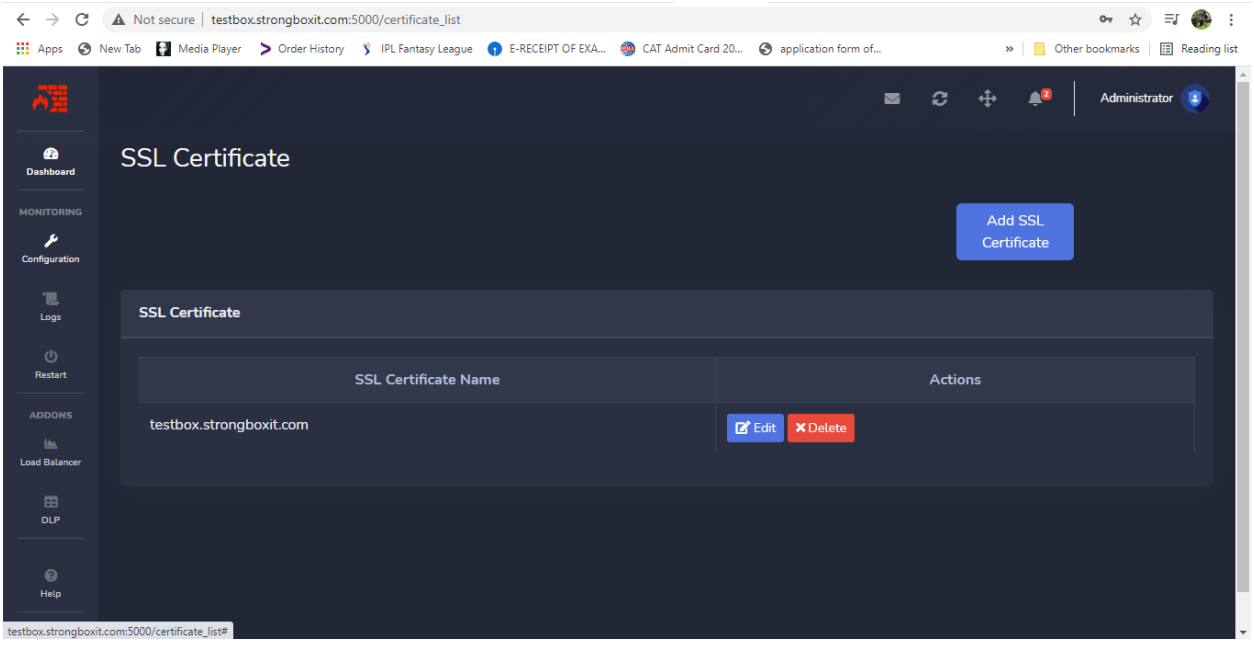
Step 5: SSL Certificate dialog box appears. You can make the necessary changes to the certificate based on your requirements



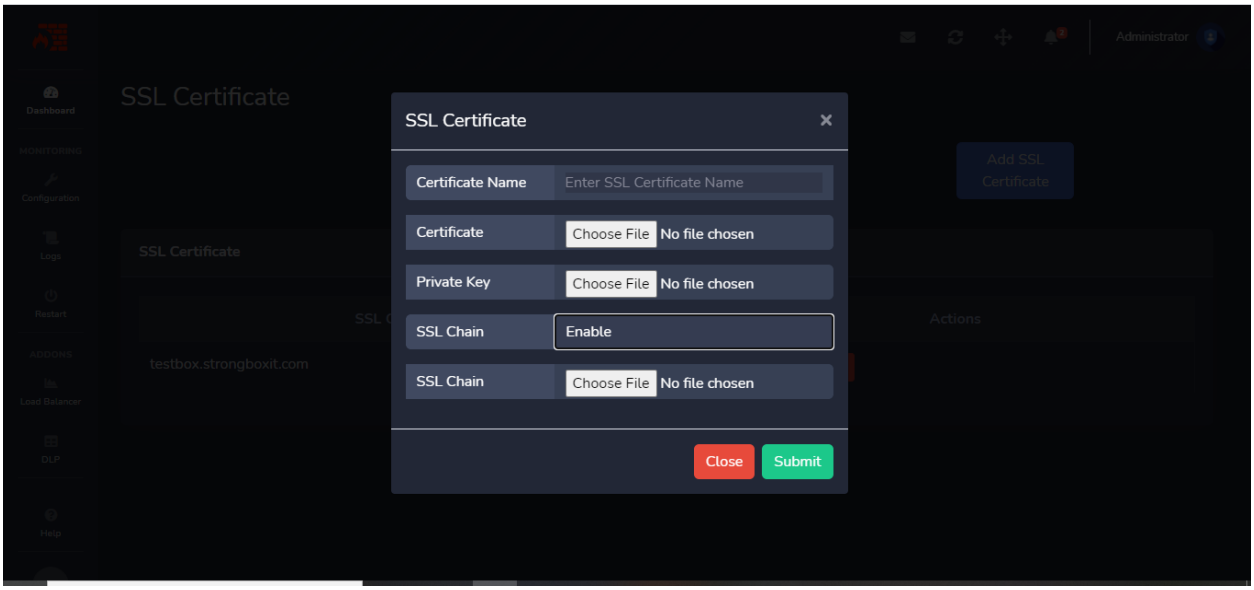
Step 6: You can delete your existing certificate just by simply clicking on the delete icon.



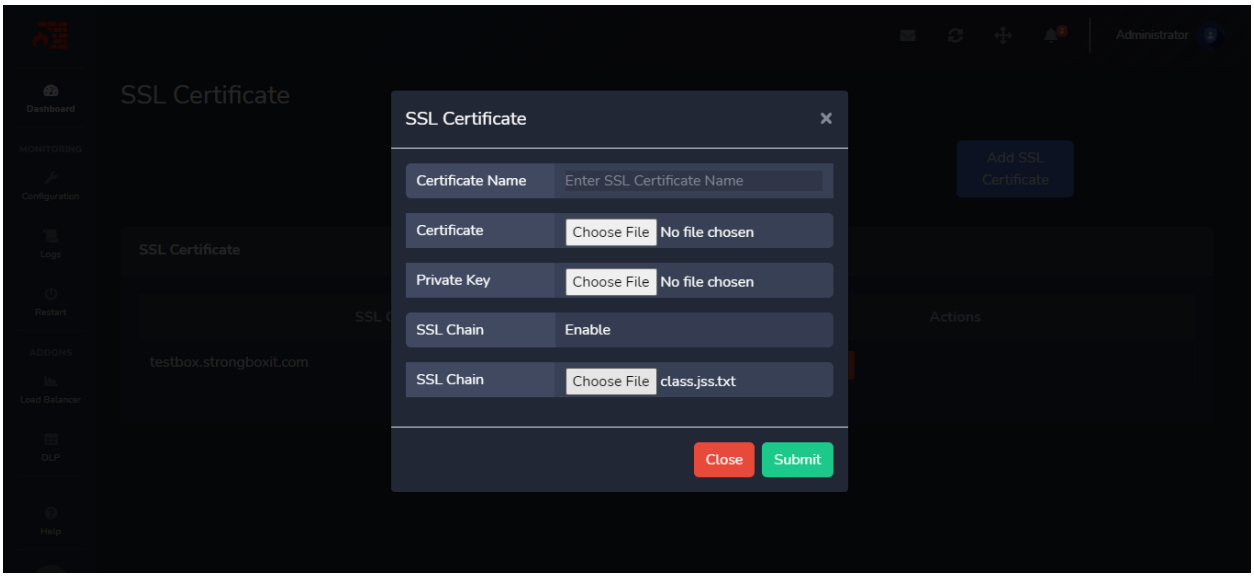
Step 7: You can also upload chain SSL certificate by clicking on Add Certificate



Step 8: SSL dialog box appears. Change the SSL chain from disabled to enabled by selecting from the drop down list box

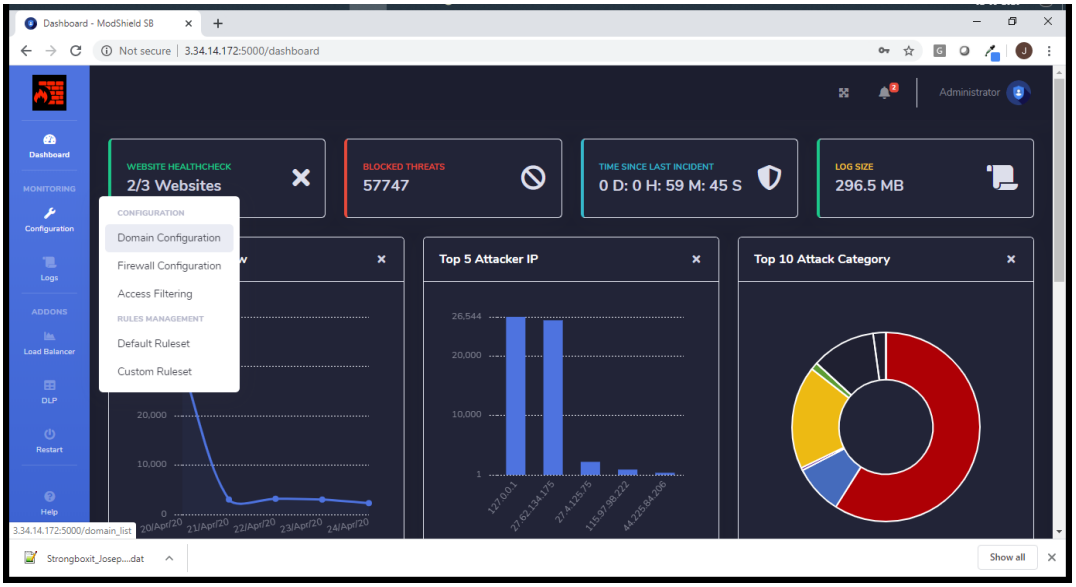


Step 9: Click on choose file option from the SSL chain column. Select the required file and then click on ok. Your file name will appear in the SSL chain column. Then click on submit.

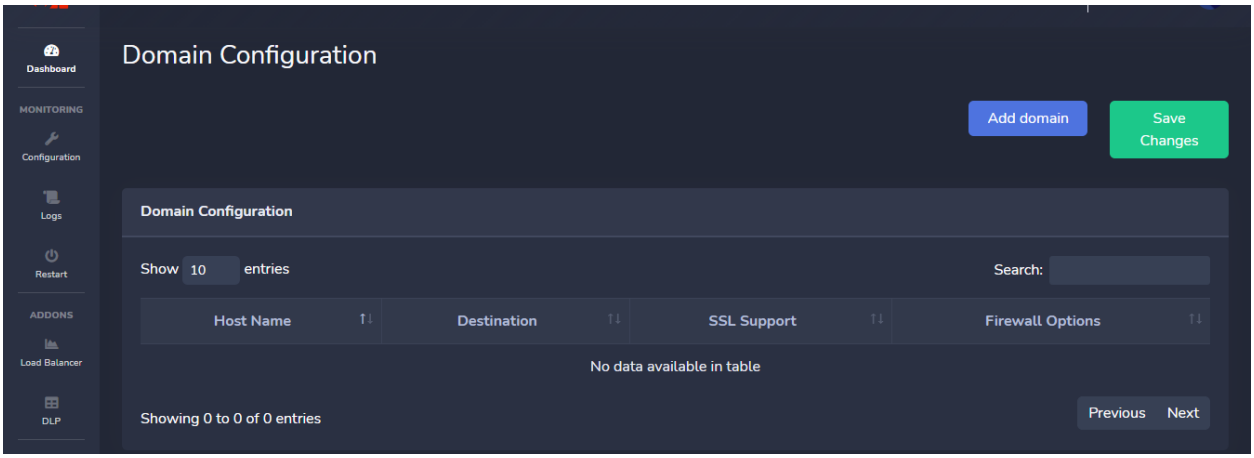


Adding a Domain to Modshield SB

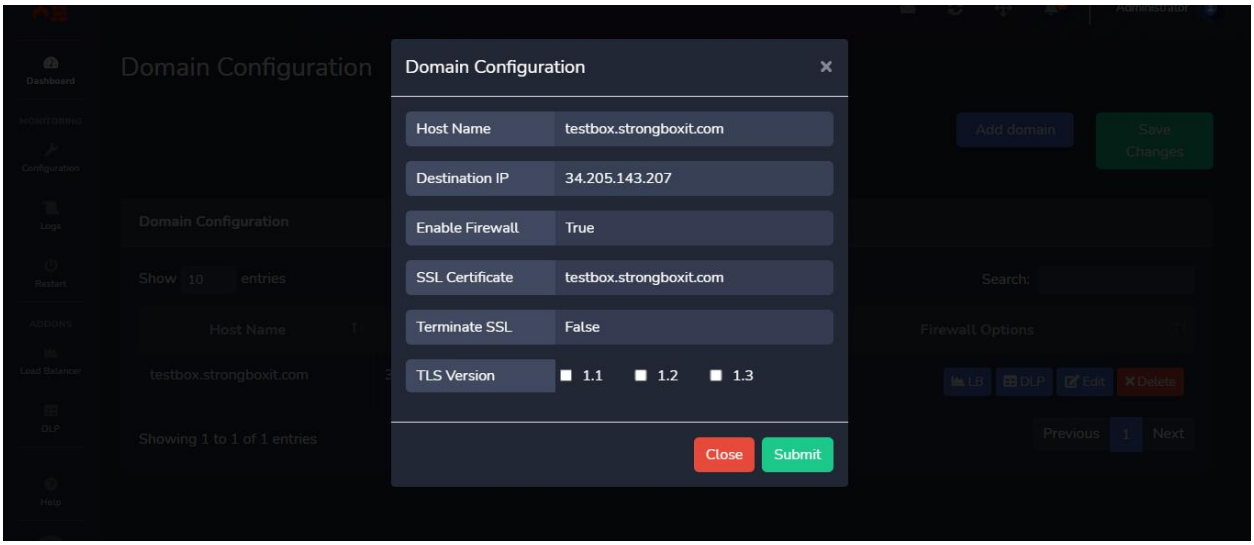
Step No: 6 To add your domain to Modshield, open the domain configuration option from the configuration menu



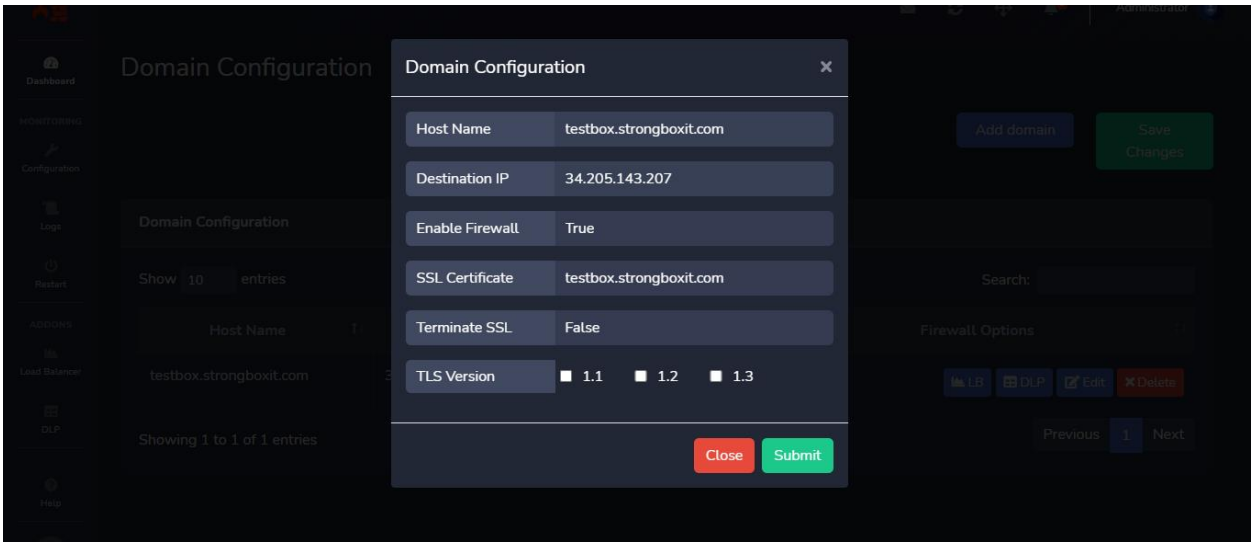
Step No: 7 Click on Add domain icon to add the domain.



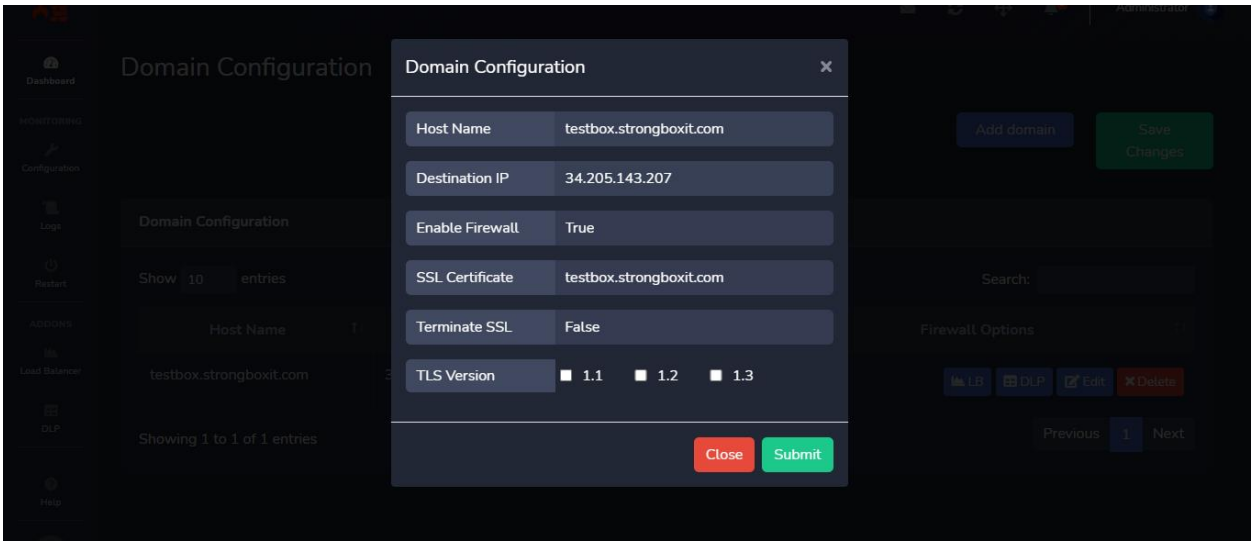
Step No: 8 Add domain dialog box will be opened to aid the configuration.



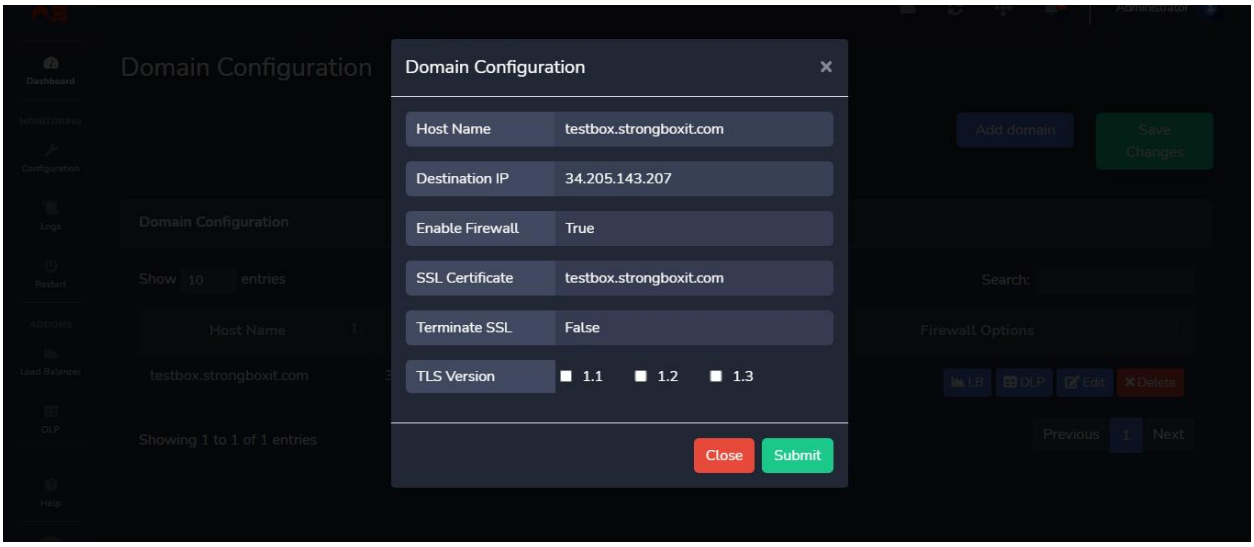
Step No: 9 Enter your domain name in the Host Name.



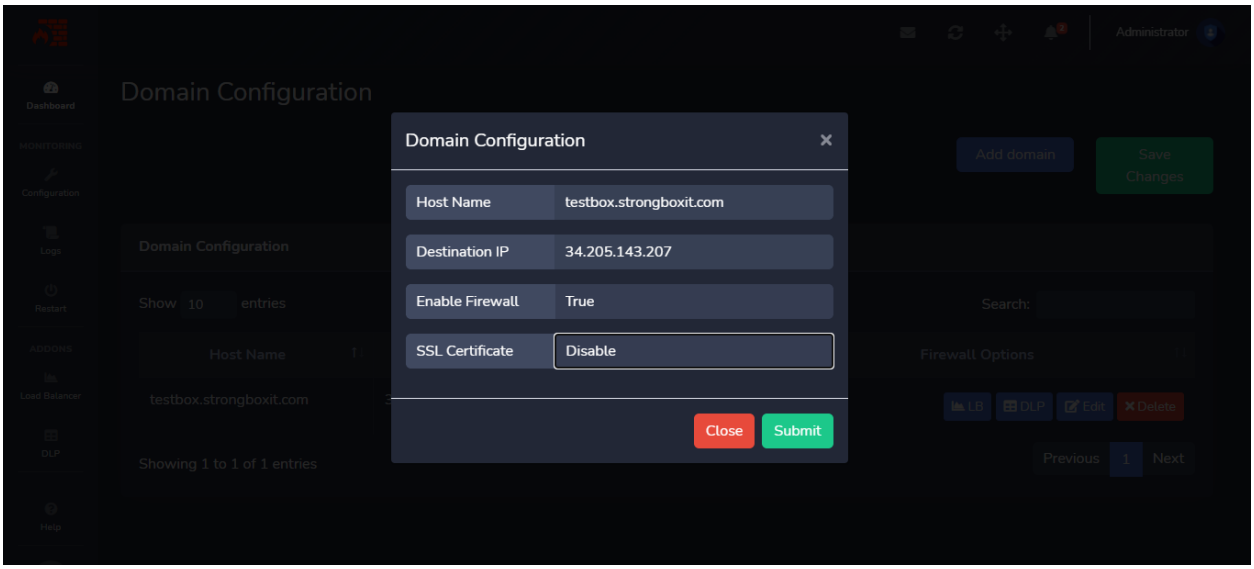
Step No: 10 Add the IP address in which the application or website is hosted



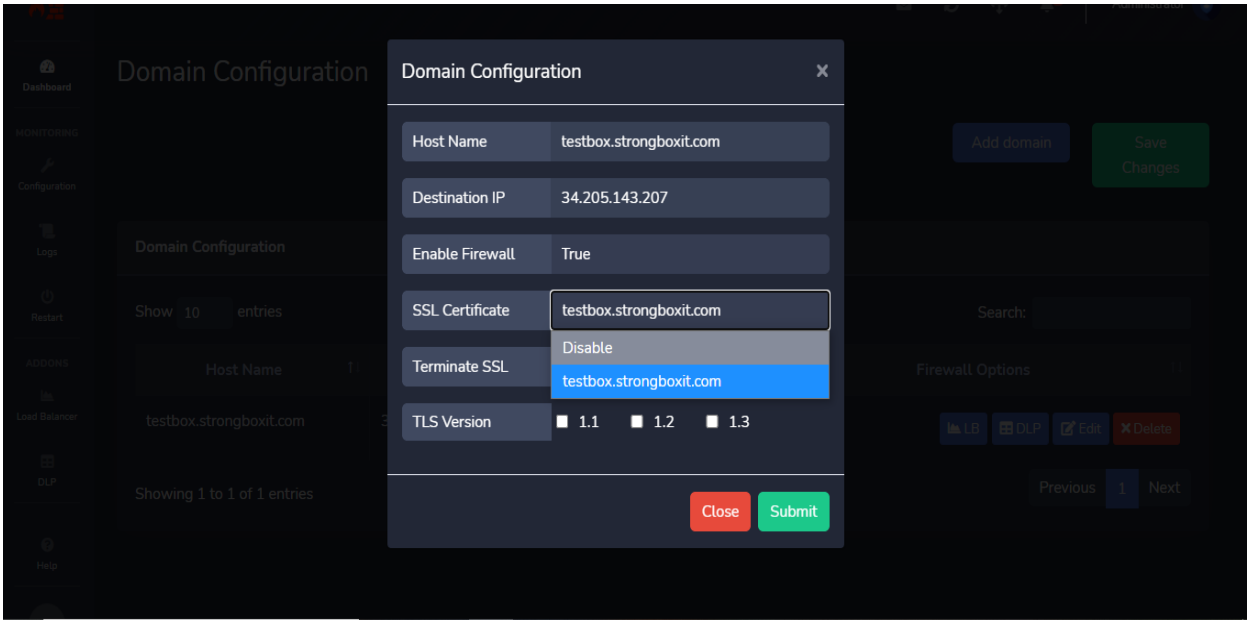
Step No: 11 Enabling Firewall will turn on protection for your domain. You can also choose to turn this on later



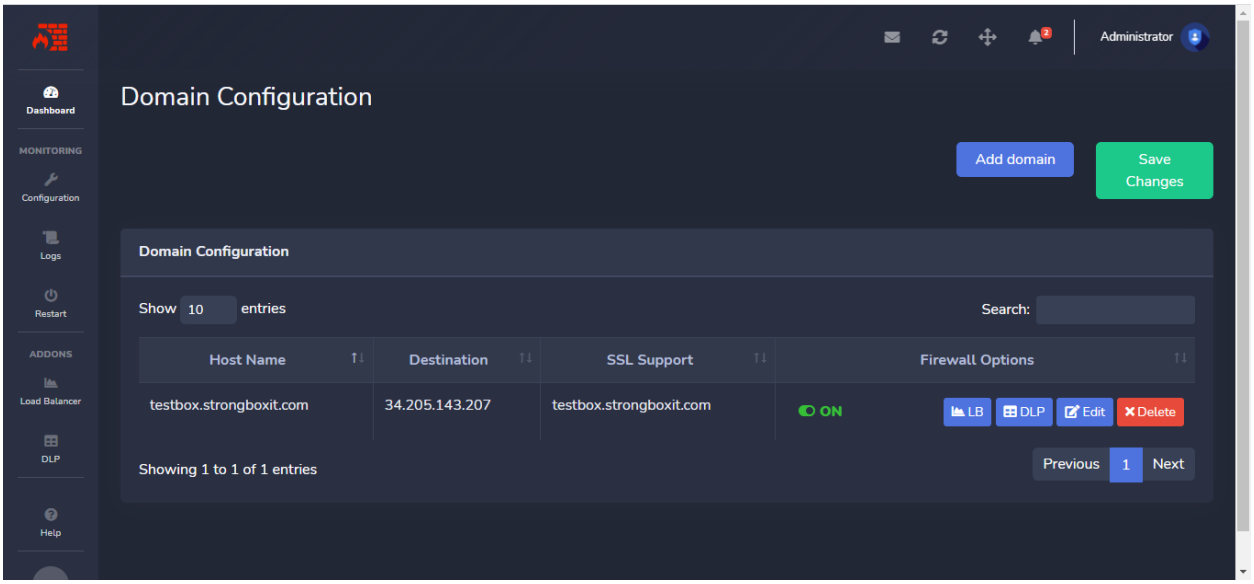
Step No: 12 If you are running a HTTP domain, click on Add Domain to complete the configuration



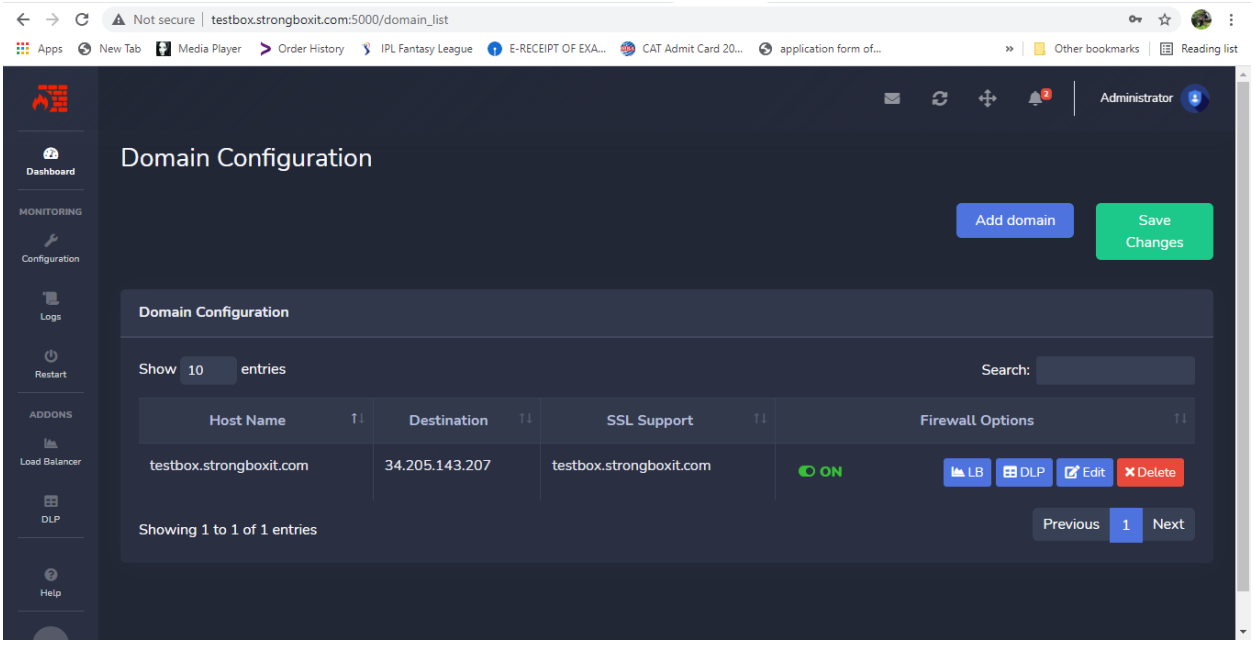
Step No: 13 If you have previously added SSL certificates, It will be displayed in the SSL certificate column.



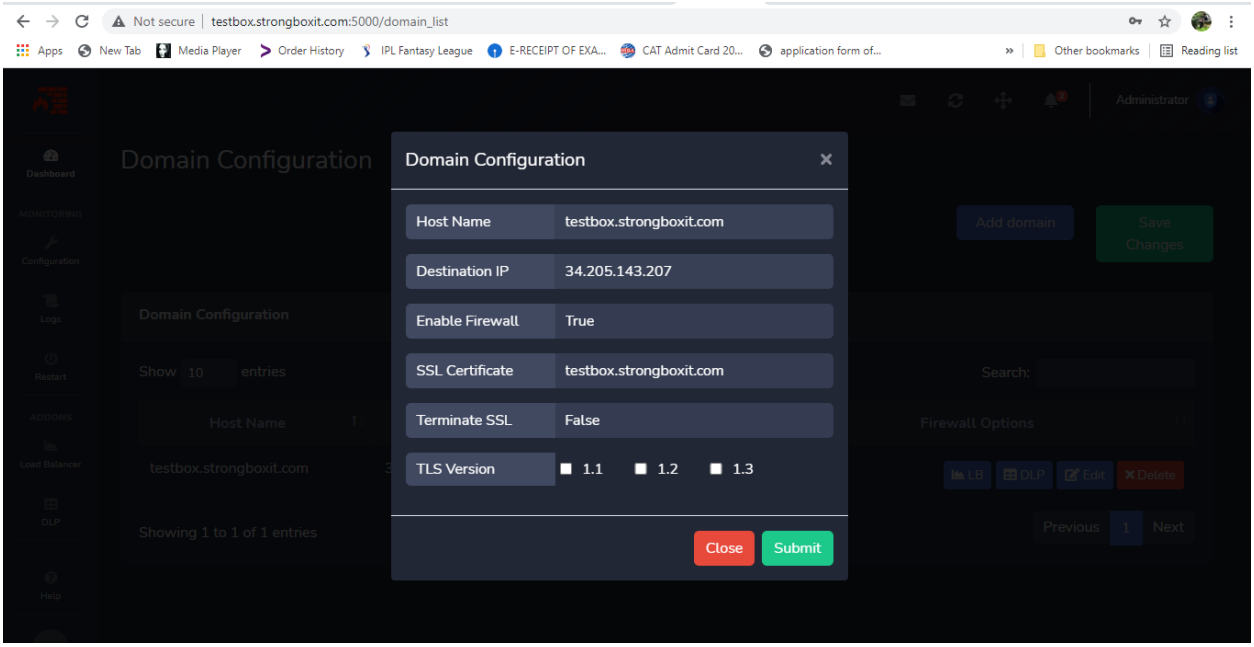
Step No: 14 You can see that the domain is now added to the list of domains



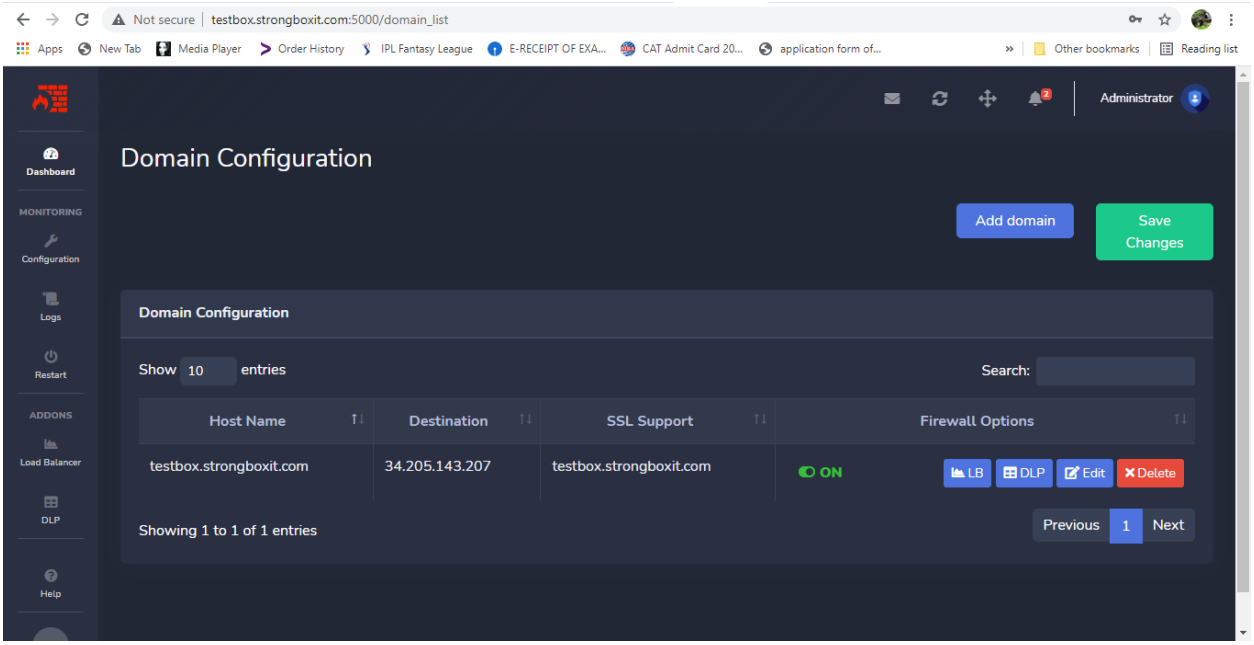
Step 15: To make changes to the domain configuration click on edit icon



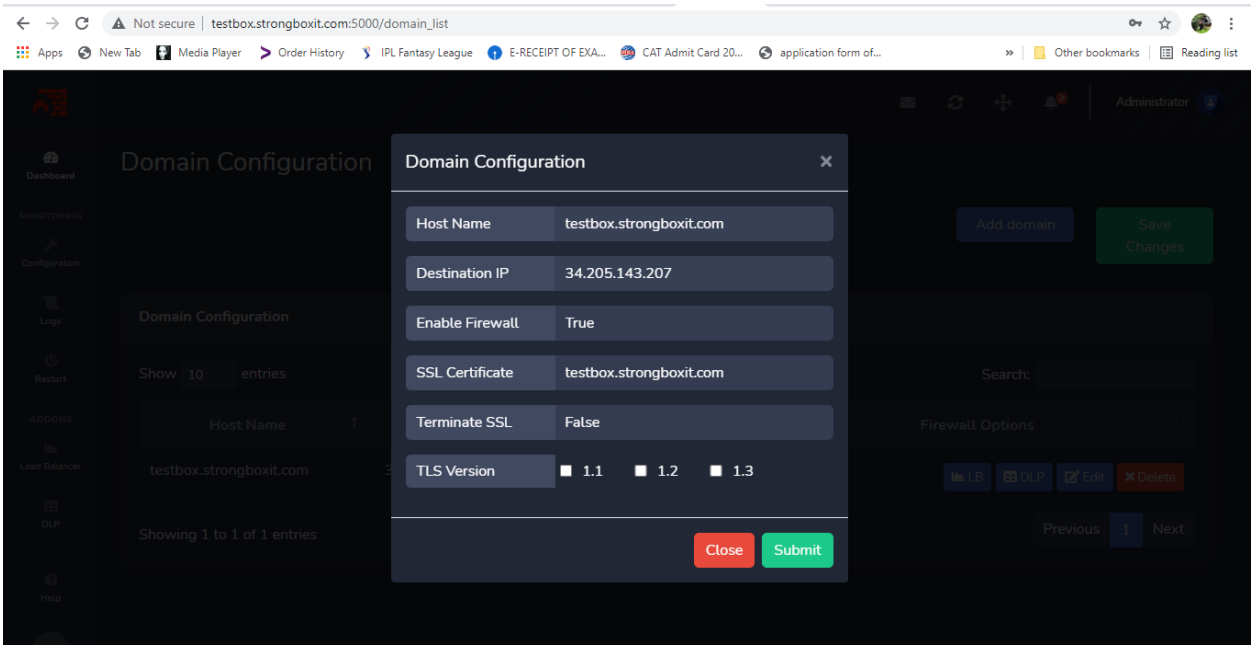
Step 16: Domain configuration dialog box appears. You can make the required changes to the DNS configuration here.



Step 17: To incorporate more than one TLS versions on your domain click on edit in the domain configuration section.



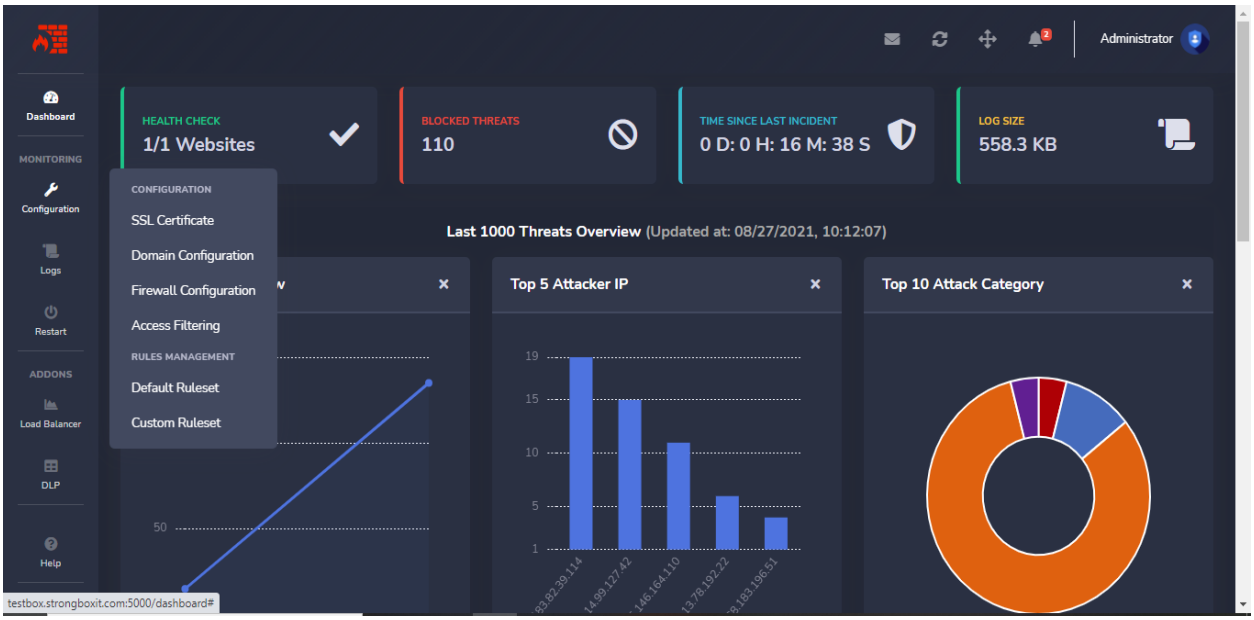
Step 18: Domain configuration dialog box appears. In the TLS versions row you can always switch between multiple versions just by clicking the checkbox next to it.



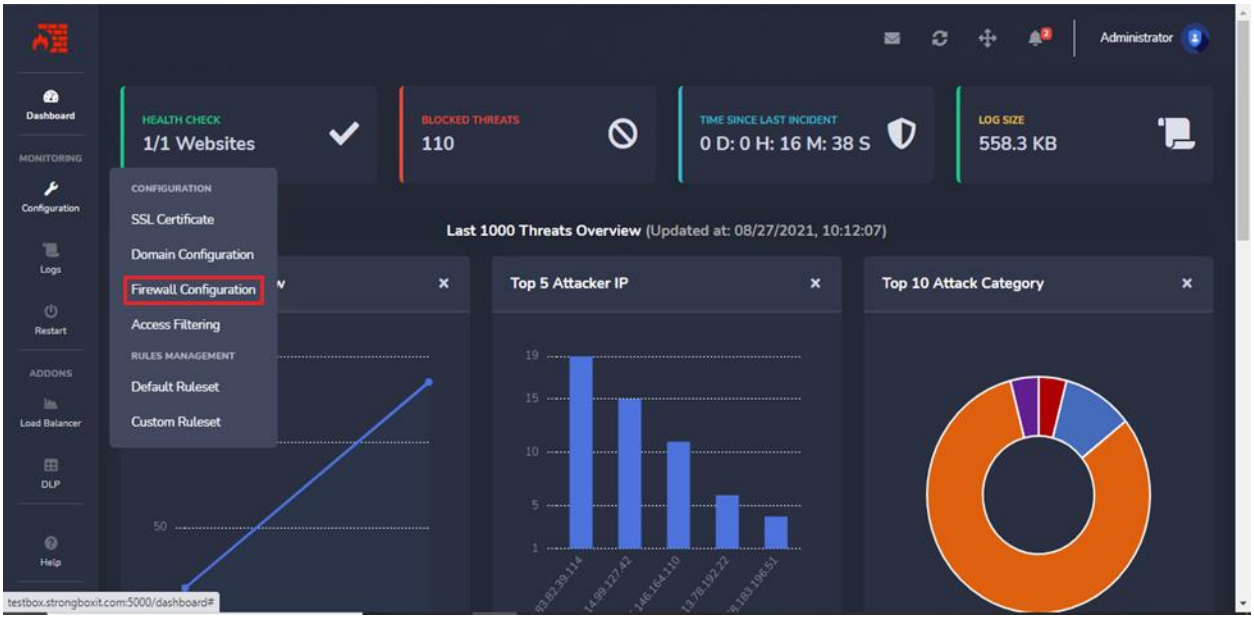
Modshield Configuration – Basic Configuration

Video Link: https://youtu.be/o-7OVKoGsp0

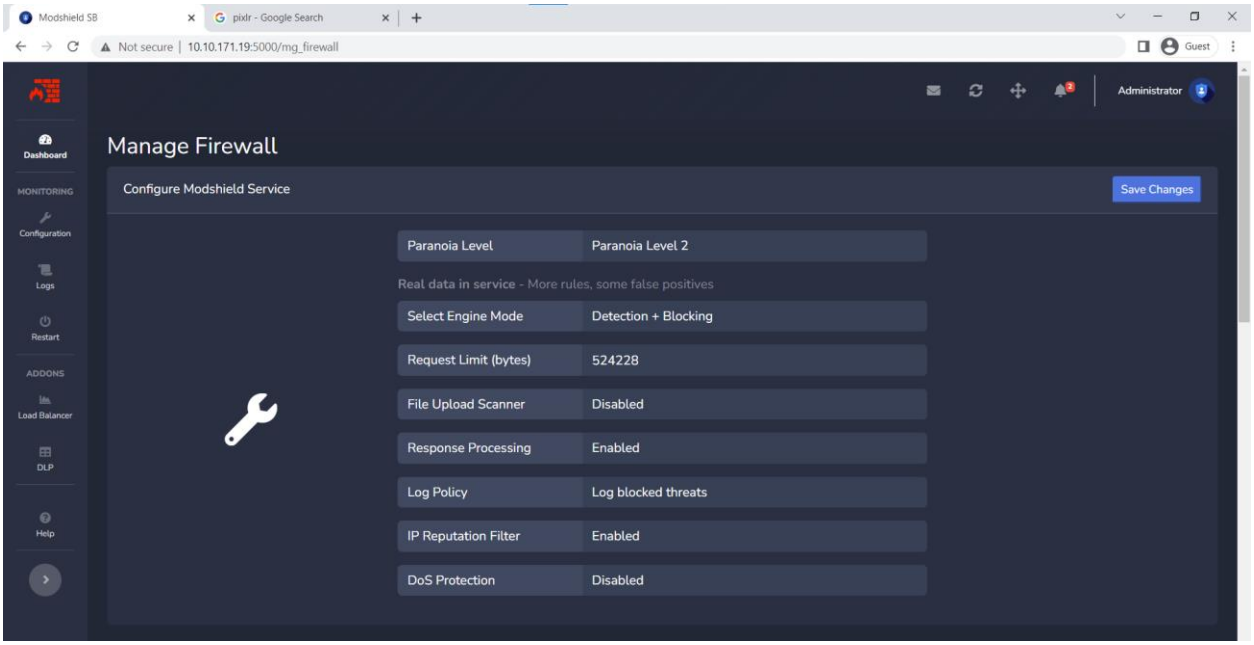
Login to your Modshield cloud instance or Virtual Machine



Select Firewall Configuration from the configuration menu

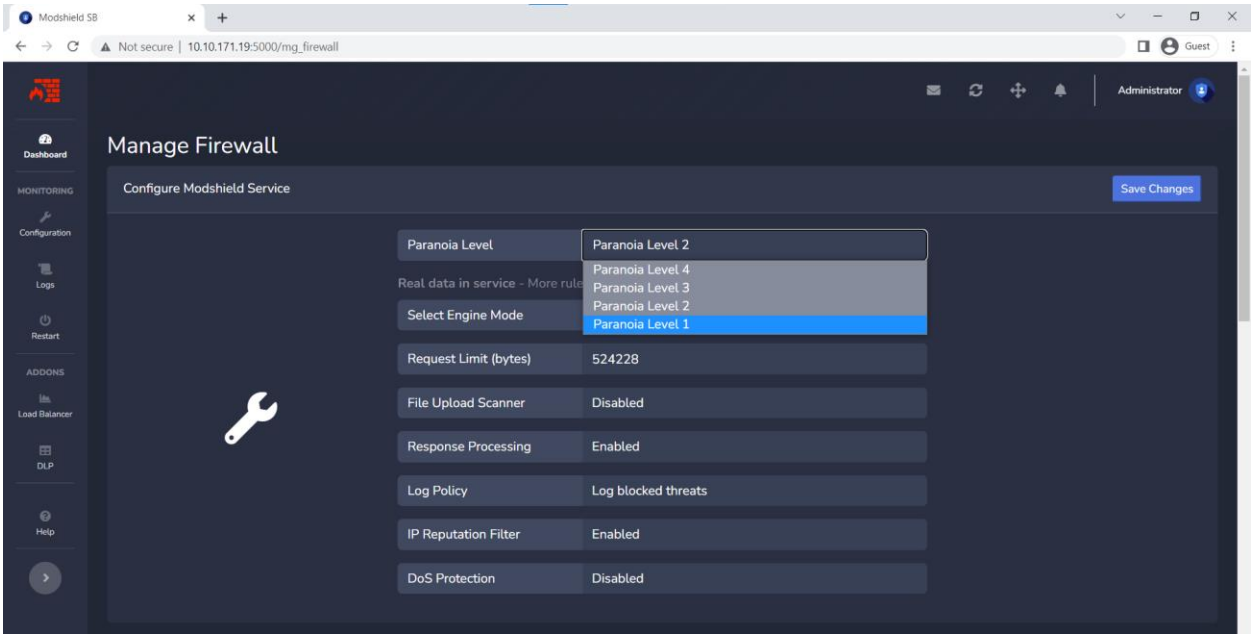


This is where you can set various options to fine tune Modhshield.

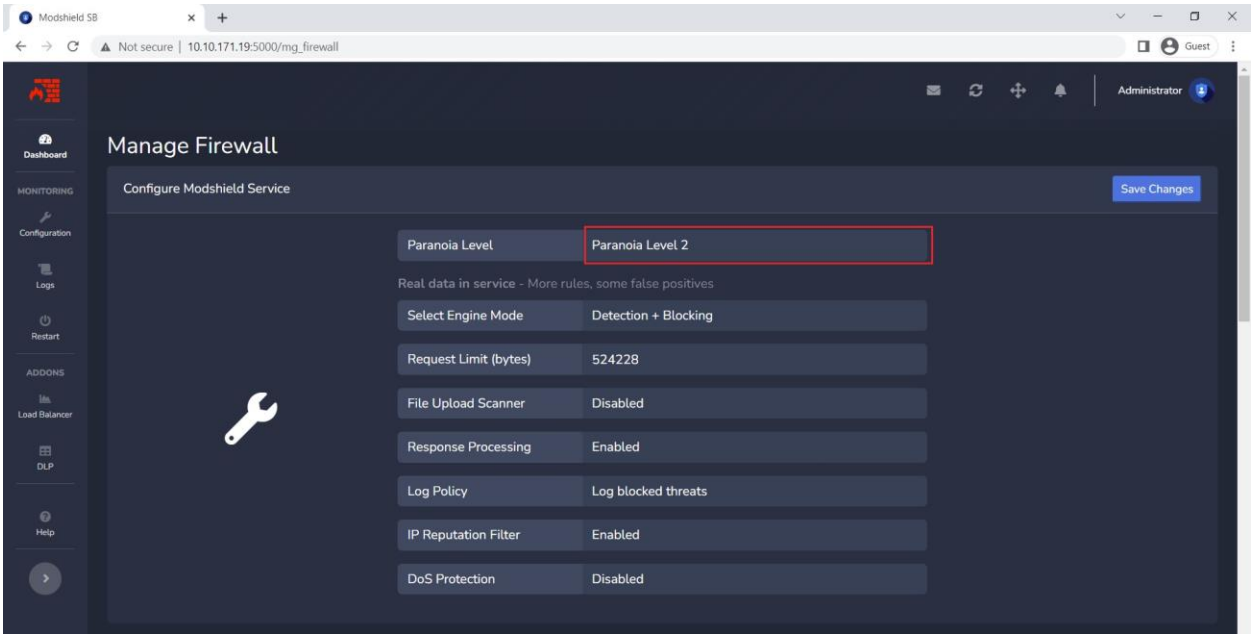


Paranoia Levels

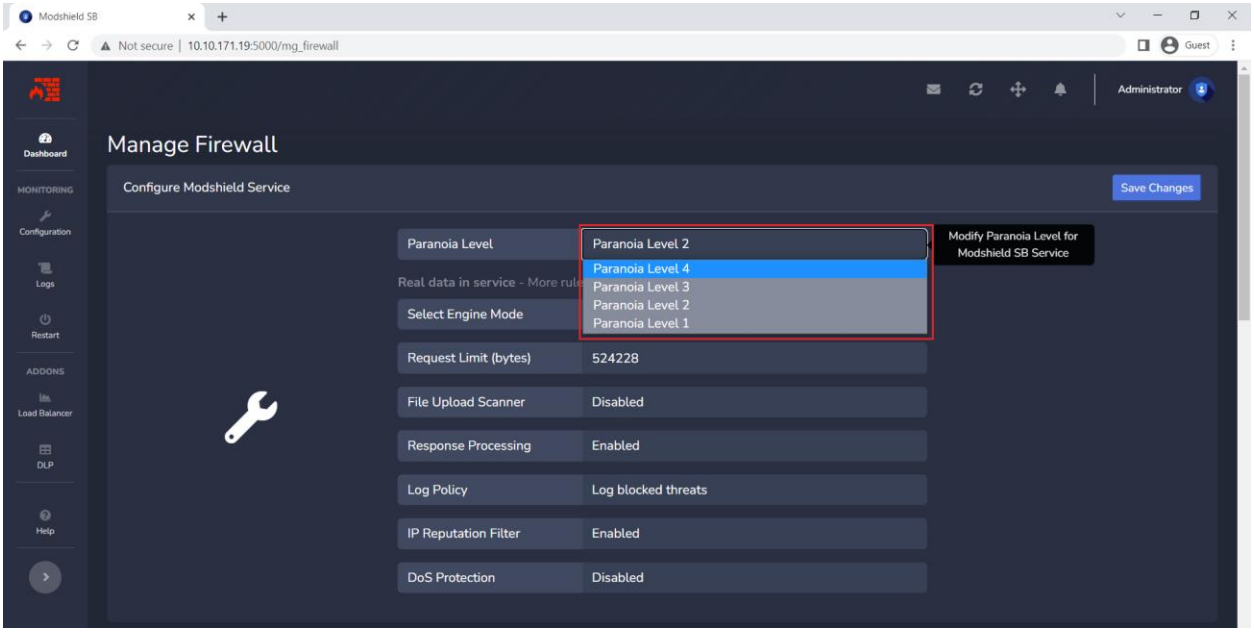
The first setting, Paranoia level, allows you to choose the tolerance level of the firewall.



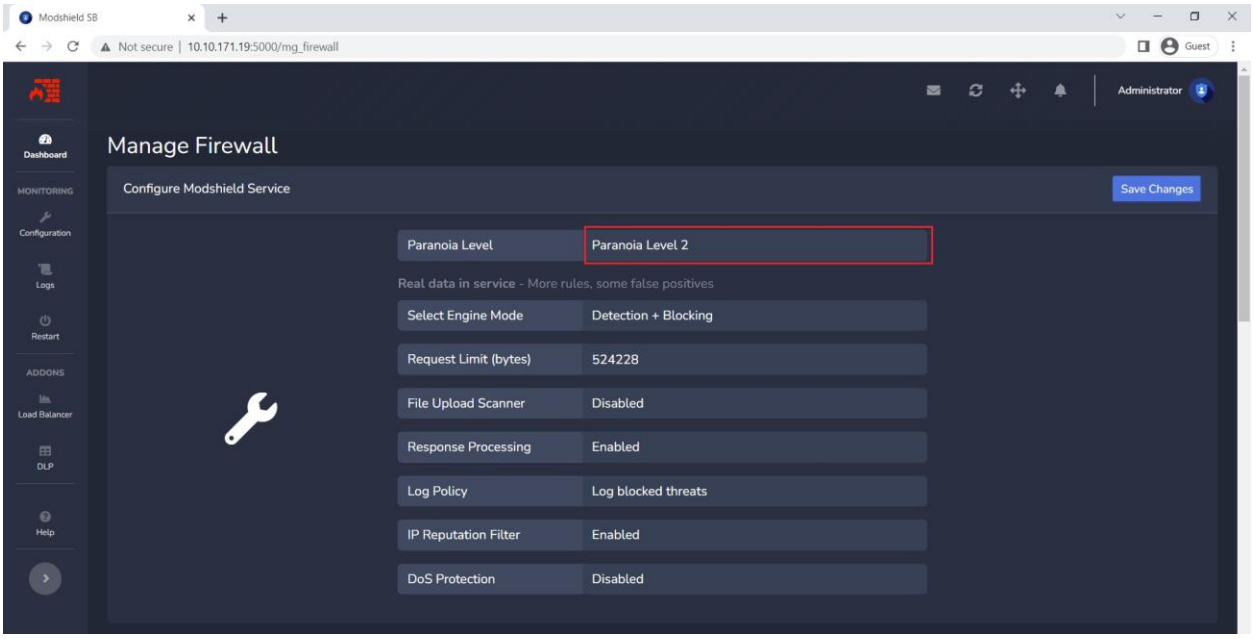
We found level 2, the default setting, to be the most effective with the least false positives



Higher the paranoia level, greater is the chance of false positives.

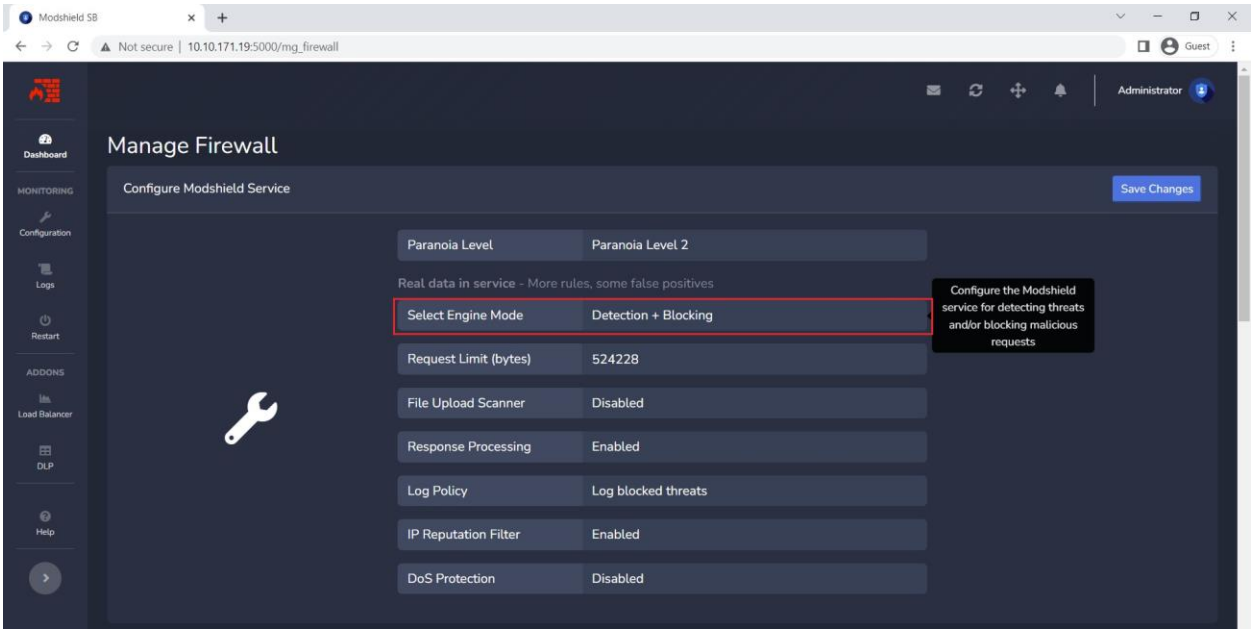


We recommend that you try multiple options before you finalise on the one that best suits your need

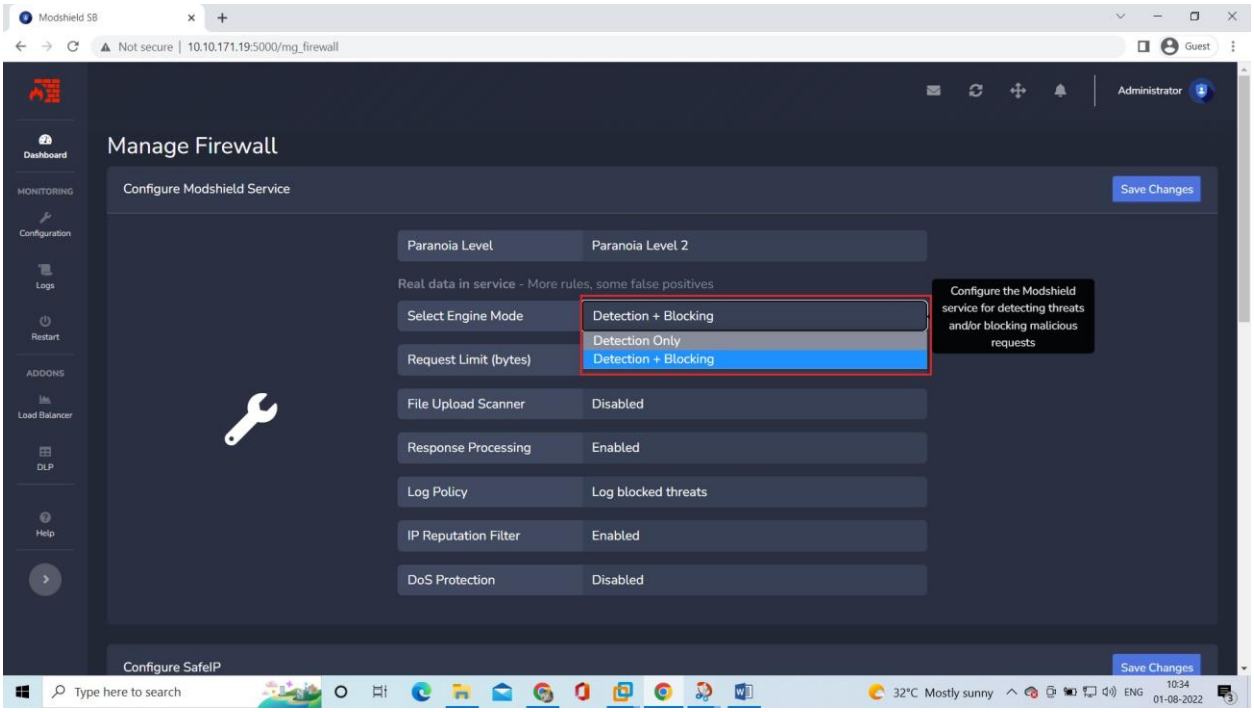


Engine Mode

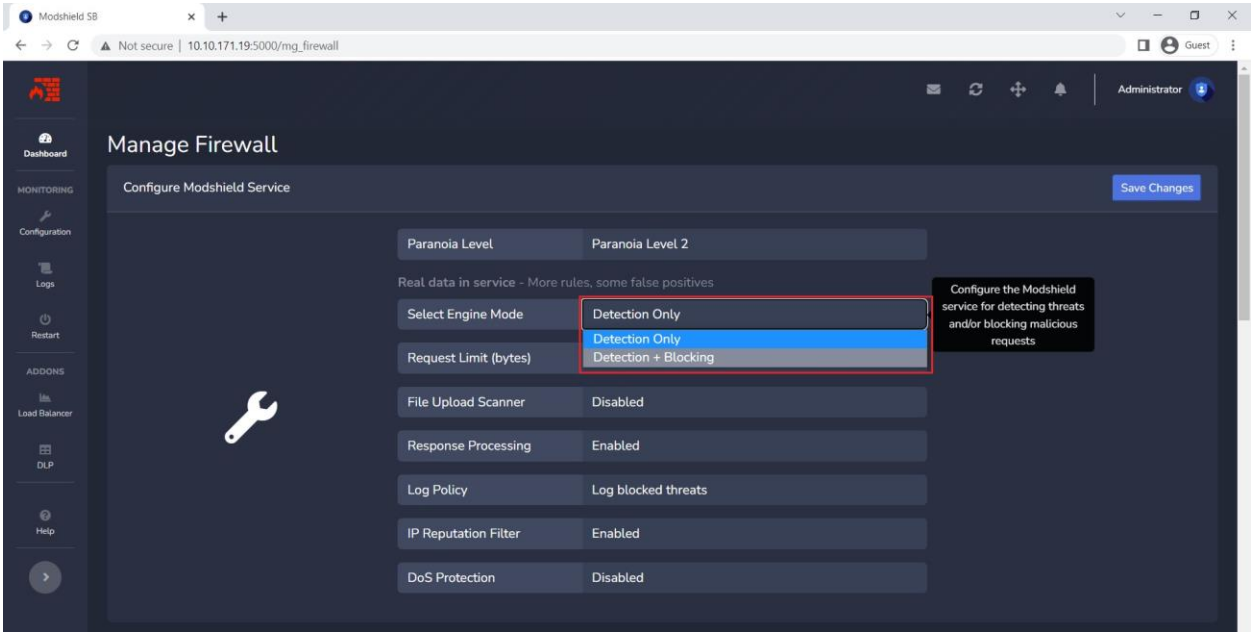
The next setting, Engine Mode, can help when you are trying multiple settings



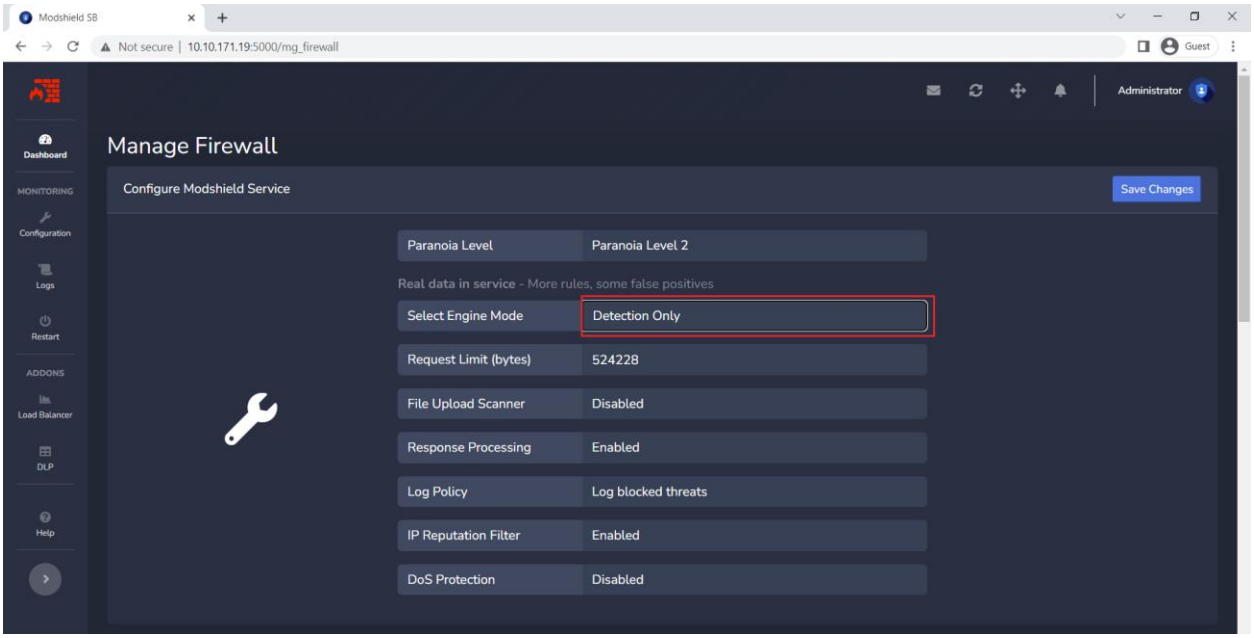
The default is Detection and Blocking. Leave this at Detection Only, till you are ready to go live



Detection only, logs all identified threats but does not block them.



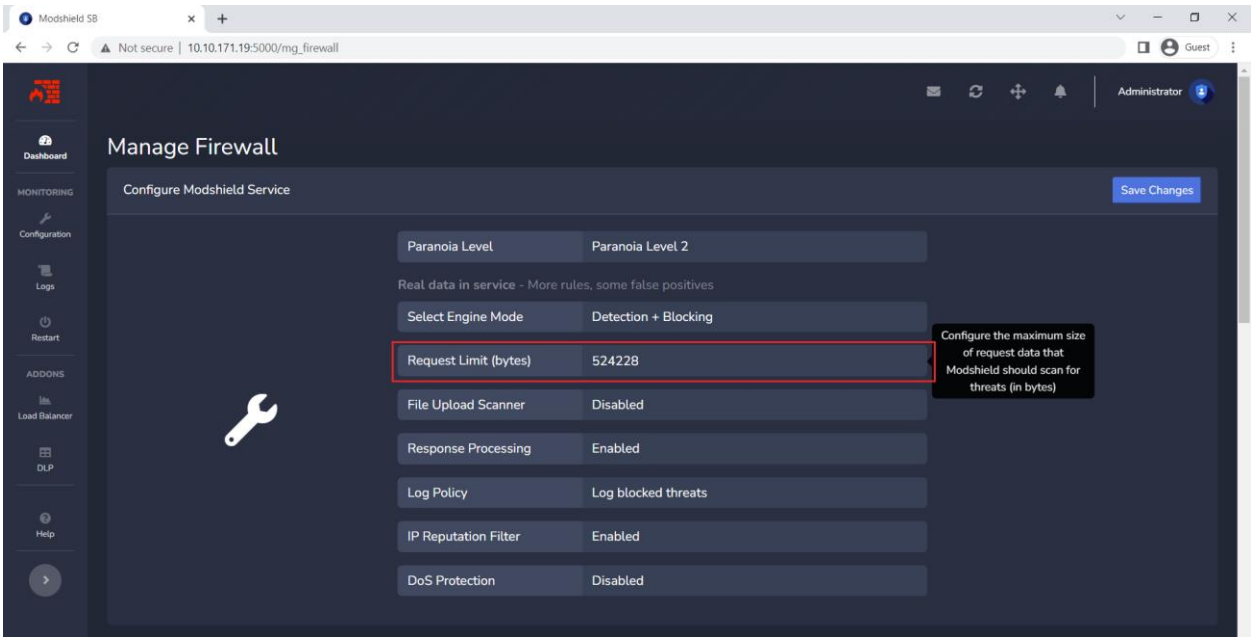
By enabling detection only you can analyze the events using this, before you instruct the firewall to block all threats.



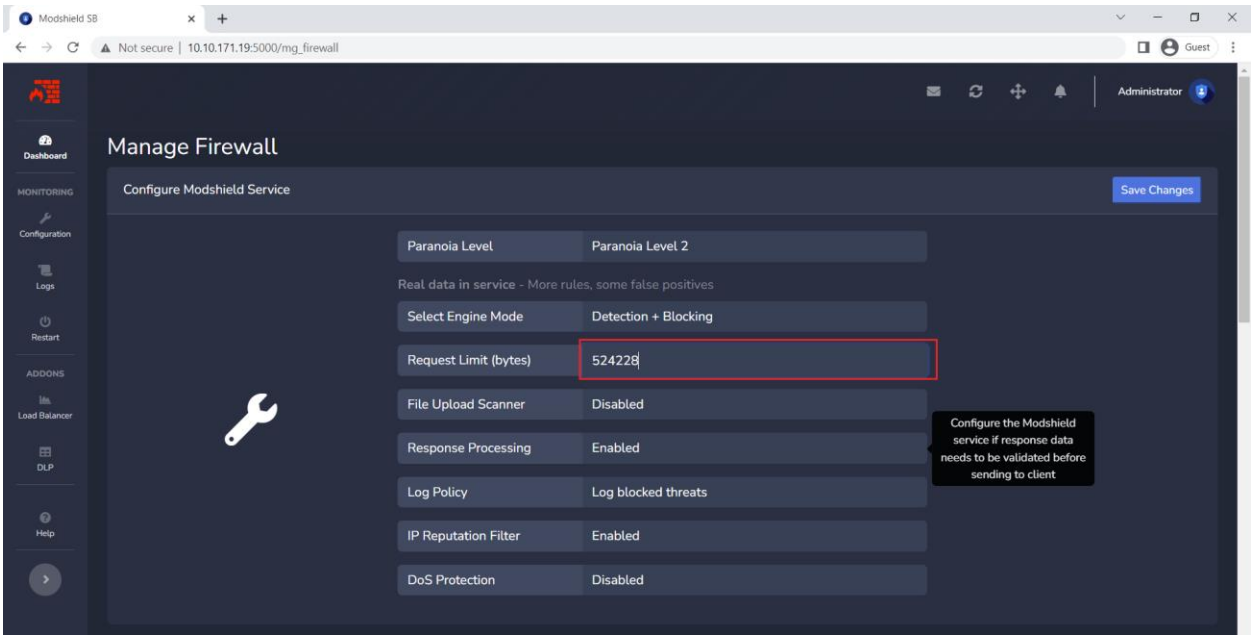
This can help in analyzing false postives, especially when you add custom rules or DLP

Request Limit

The next setting, Request limit, is the size of a request that the firewall will process.

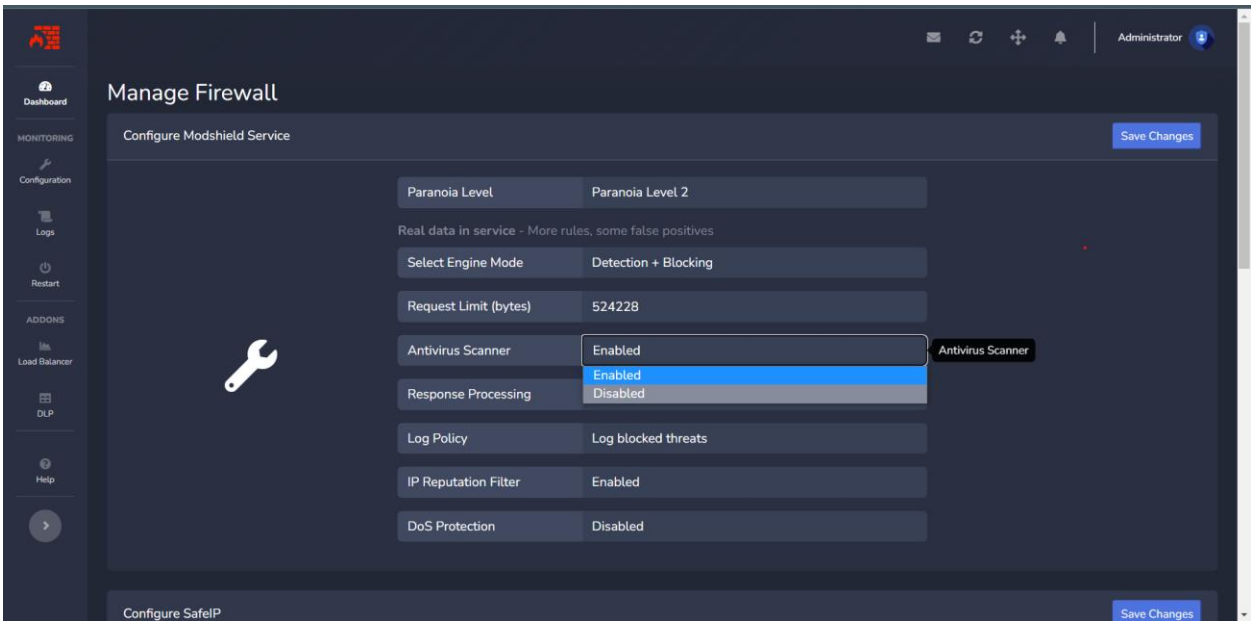


You can increase this value if you are expecting large attachments to avoid them being blocked



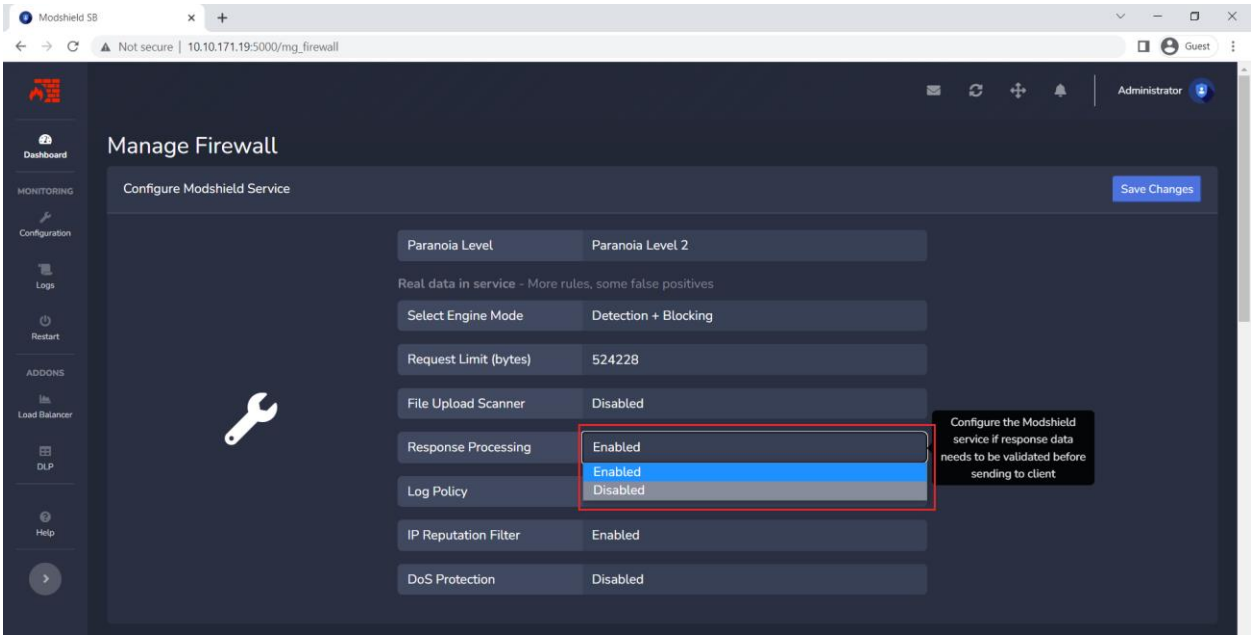
Antivirus Scanning

You have the option to enable or disable antivirus scanning. When enabled, the scanner will detect and prevent malware-infected files before they are uploaded to the application.

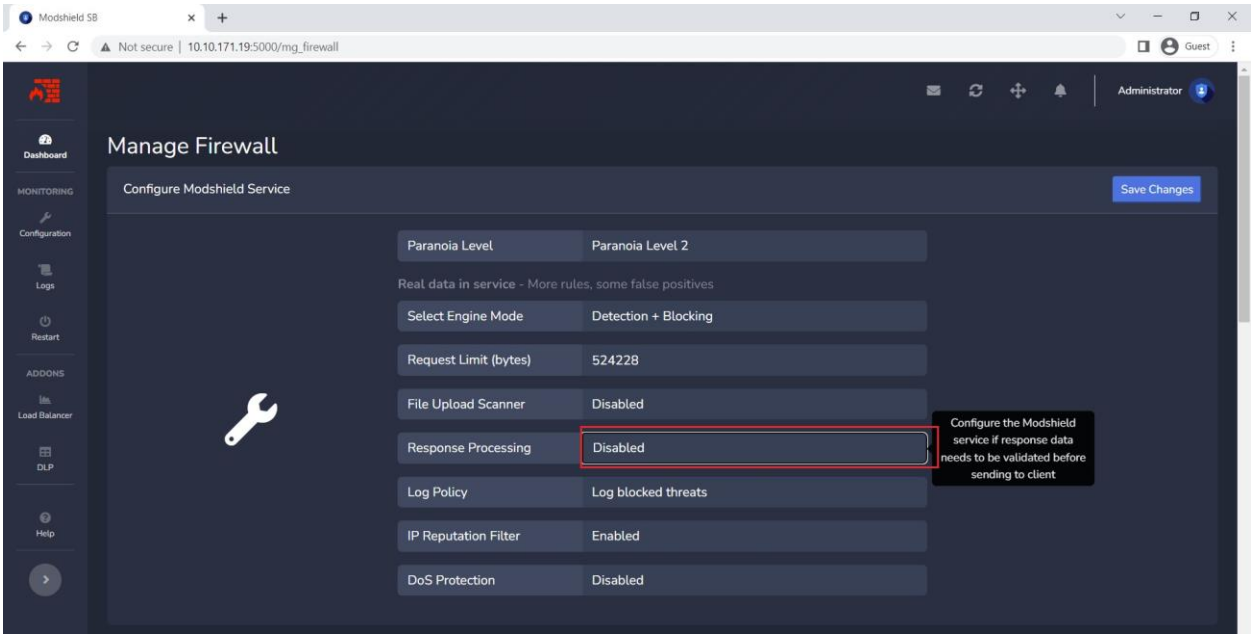


Response Processing

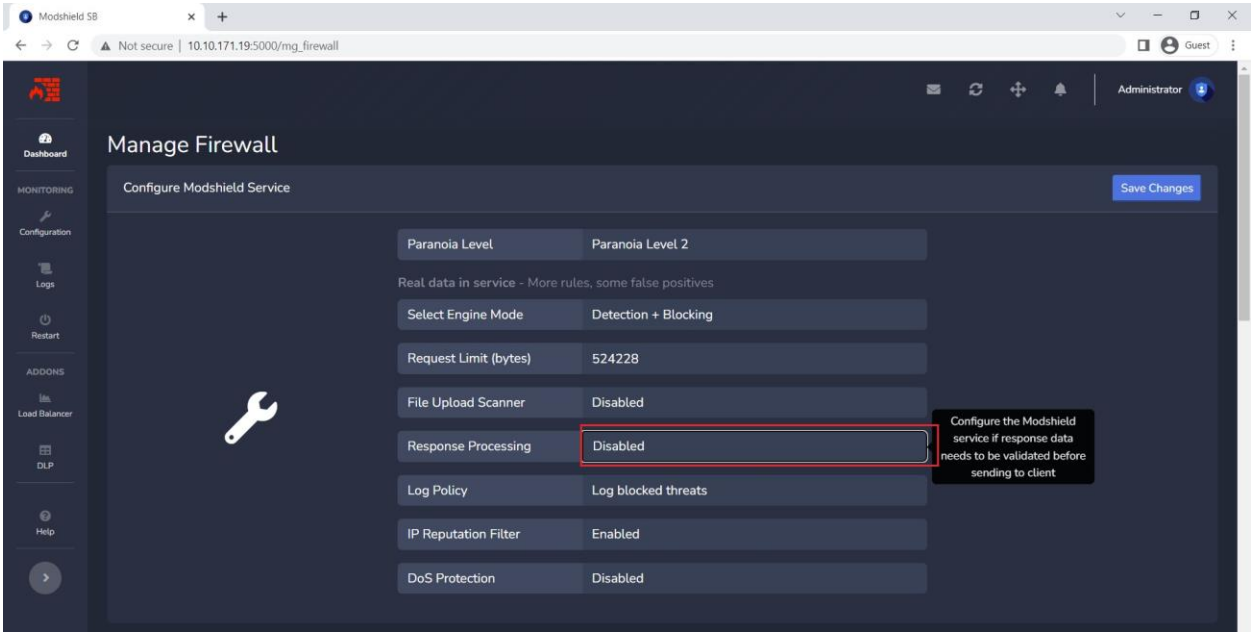
You can turn response processing on or off using this setting.



If your application responses need not be validated, you can turn this off.

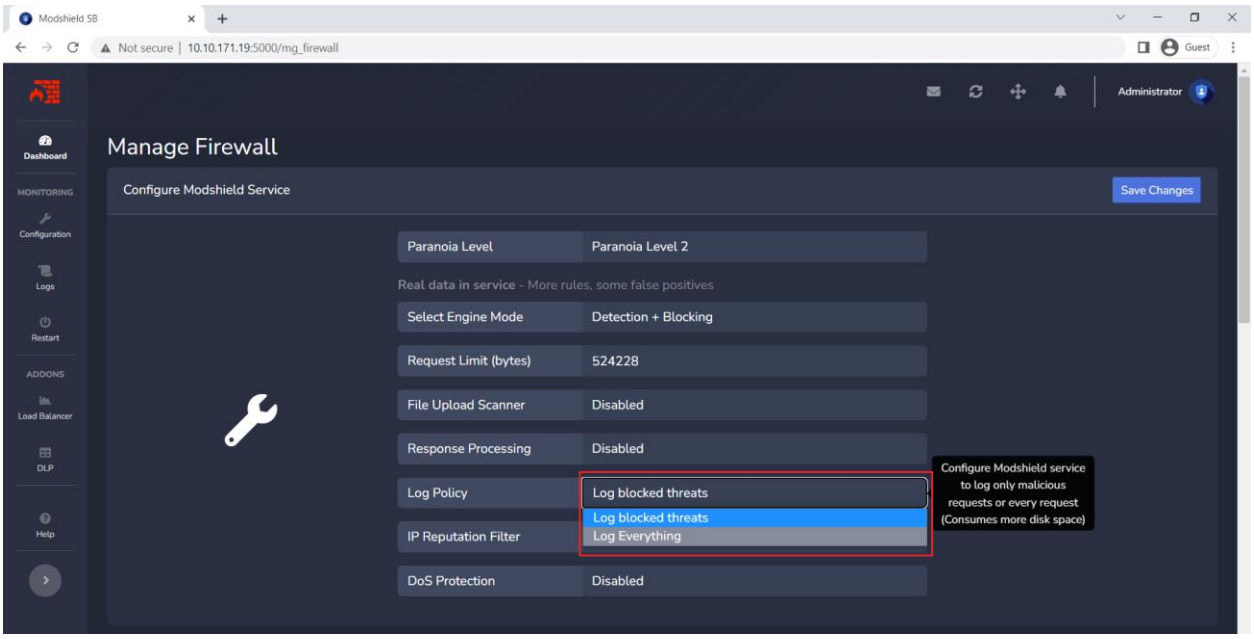


Disabling this will give you a higher performance. This is enabled by default

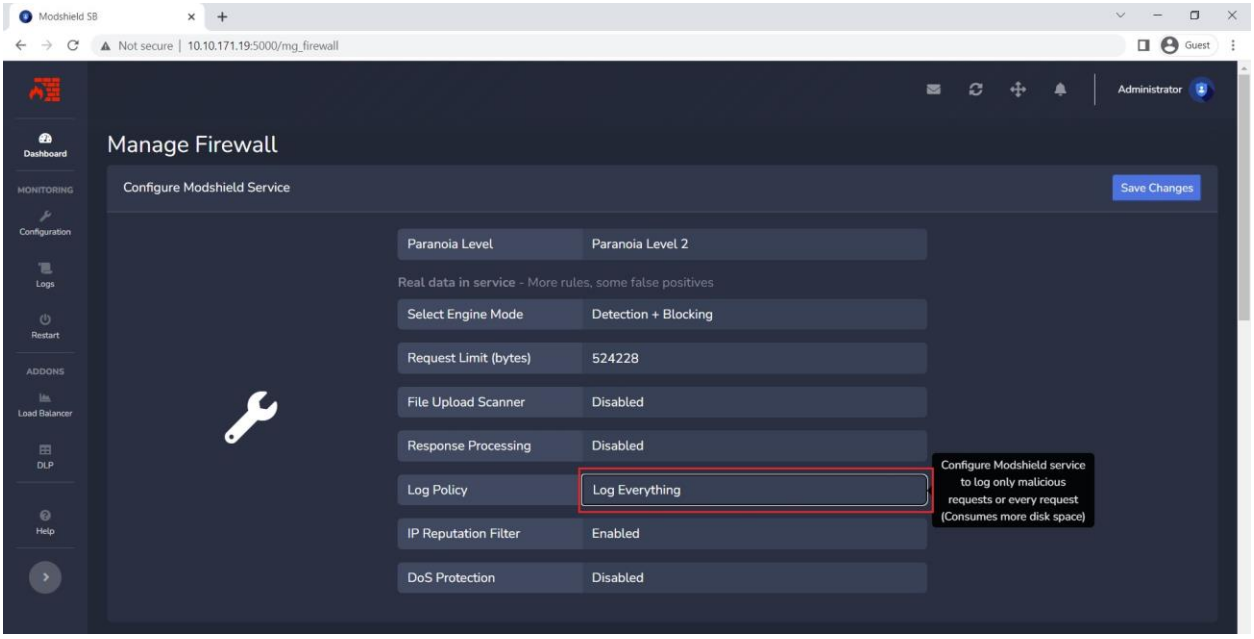


Log Policy

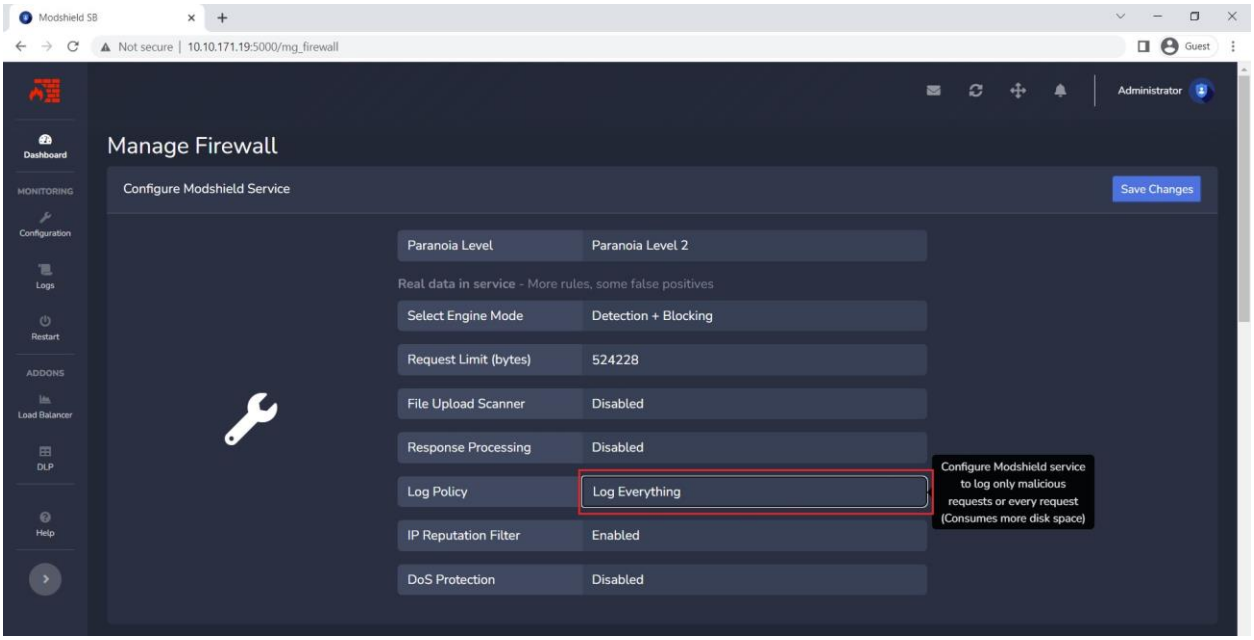
You can also choose to log only the blocked threats or log everything, based on your requirement



Logging every request and response might be required for certain compliance reasons

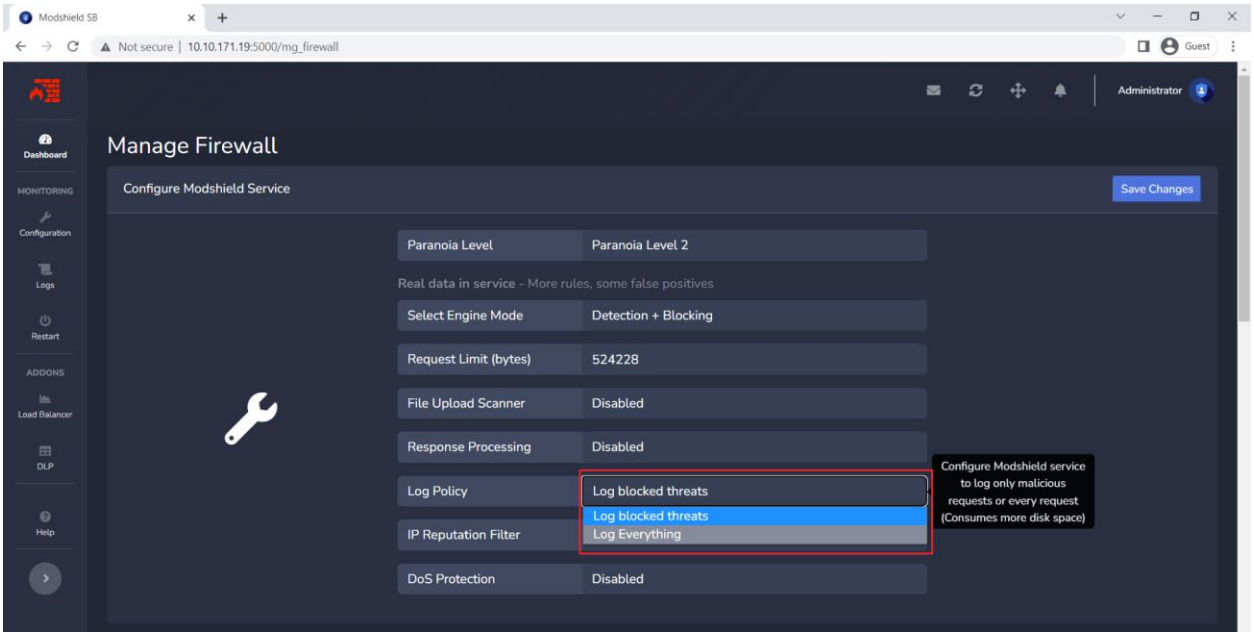


Also be aware that log files grow faster when all activity is logged.

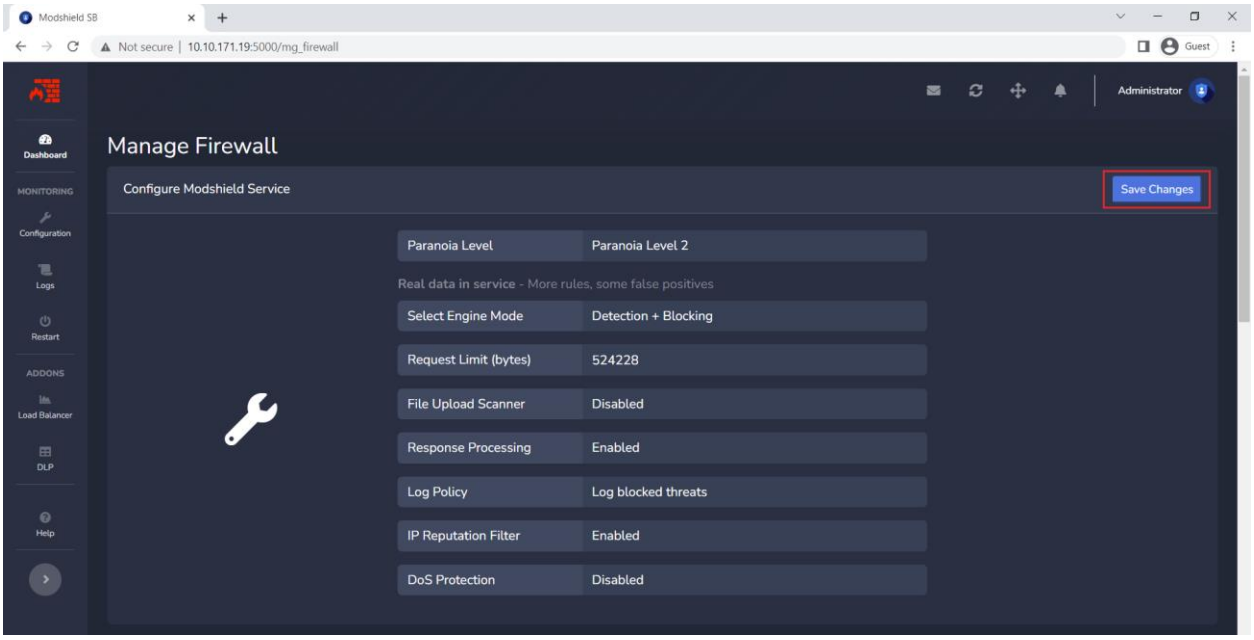


If you are forwarding log entries externally, the forwarded events are also based on this setting

The default setting is to Log only the blocked threats.



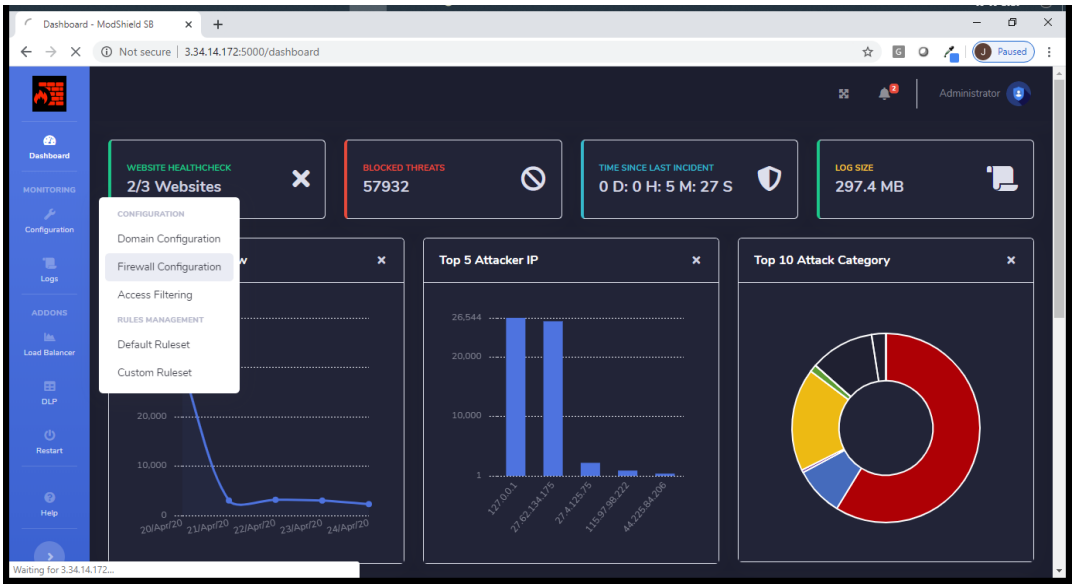
Please remember to Save Changes for all your settings to take effect



Modshield Configuration – Fine tune your firewall

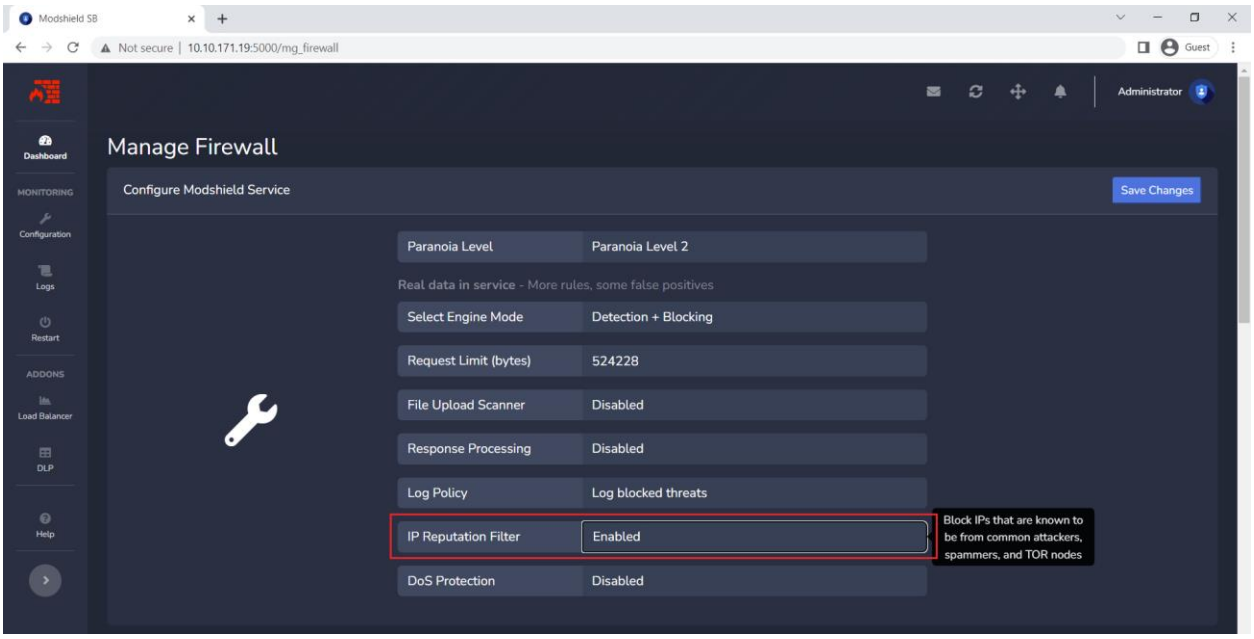
Video Link: https://youtu.be/rfLHrQibYdc

Select **Firewall Configuration** from the configuration menu

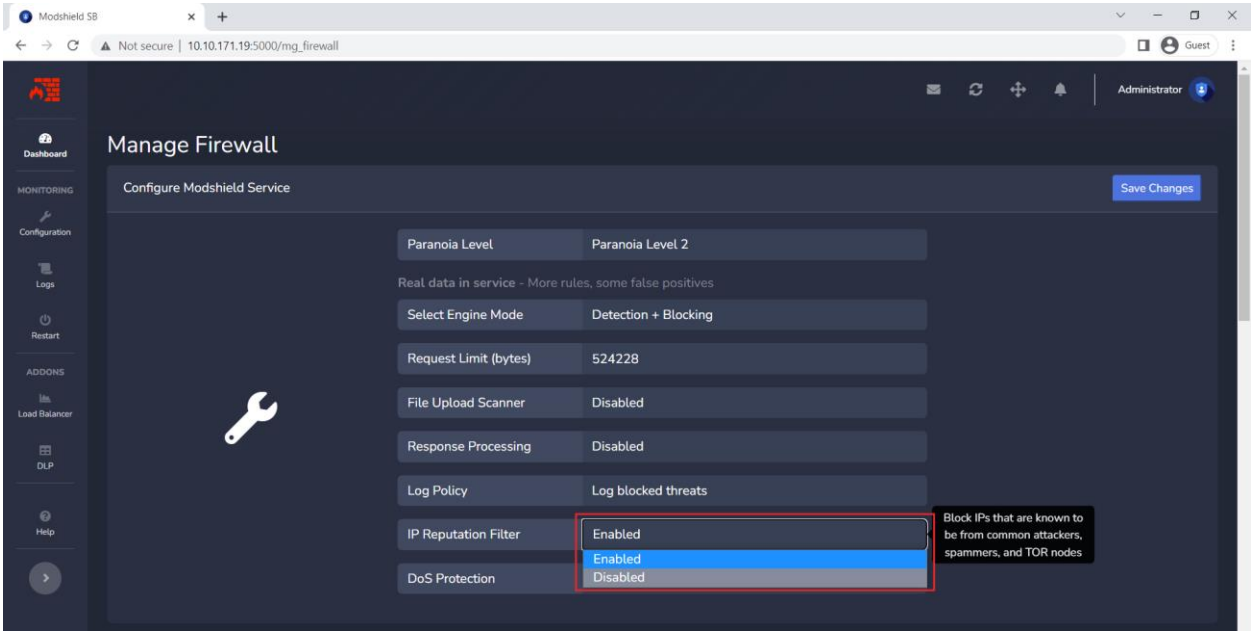


IP Reputation Filters

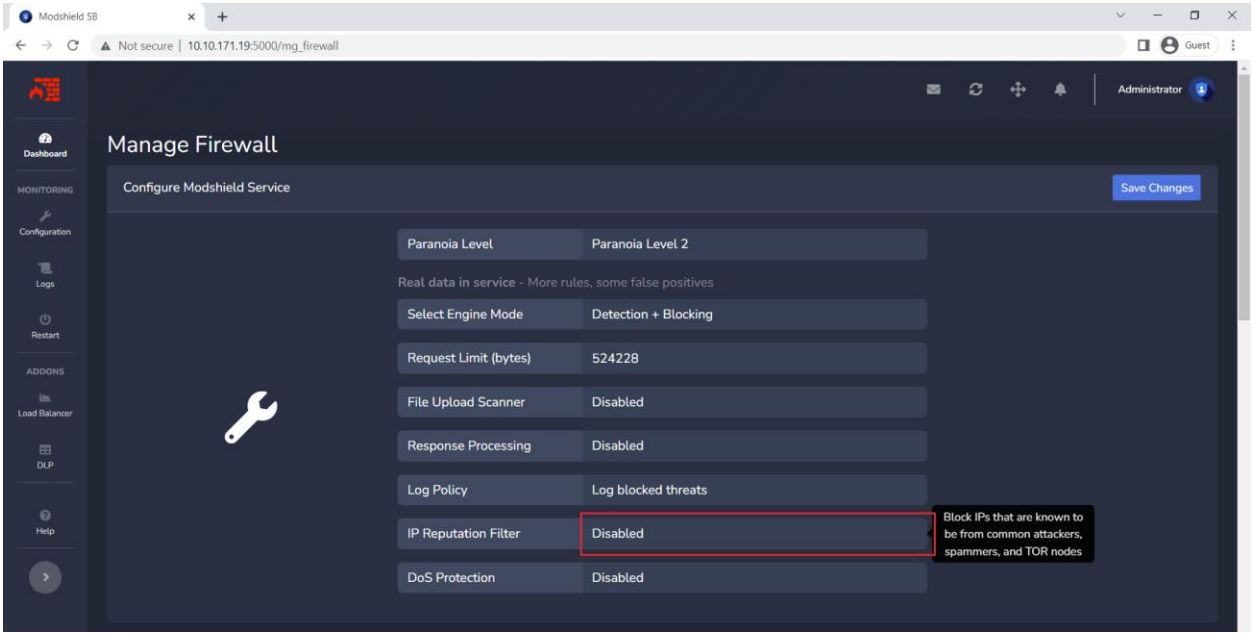
The first setting that we will look at, is IP reputation



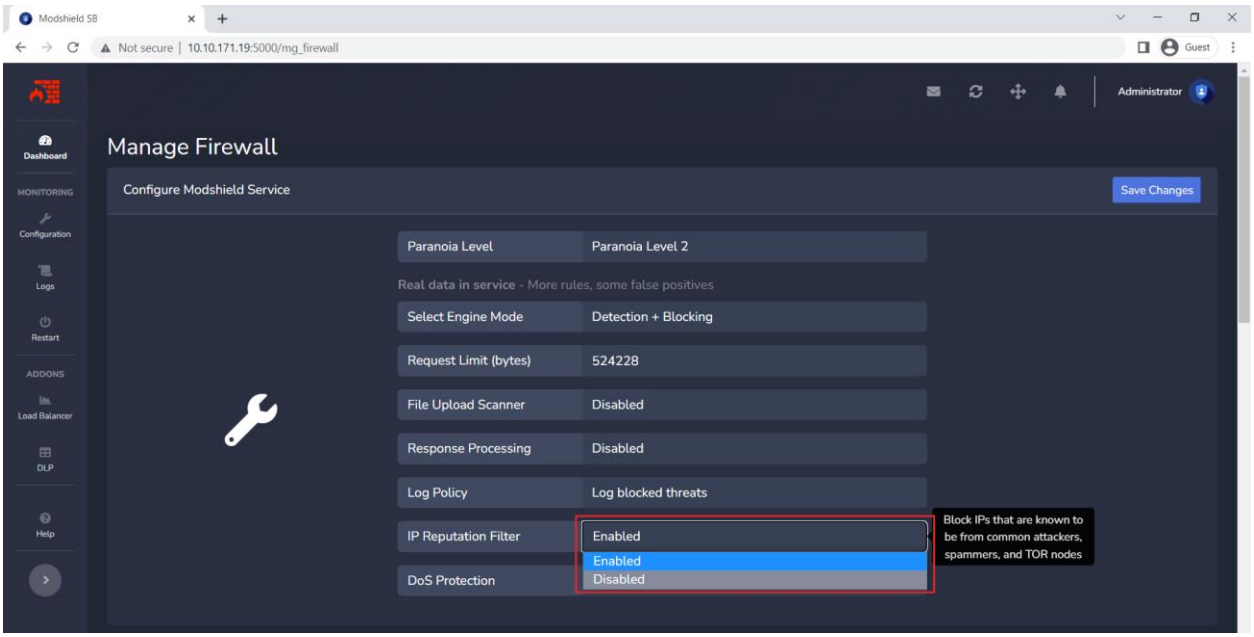
This filter blocks all known bad IP addresses, Bots, crawlers and Tor exit nodes



Modshield is continuously updated with threat intelligence feeds to ensure efficient detection



The default setting is "Disabled". Enable it to have real time threat protection

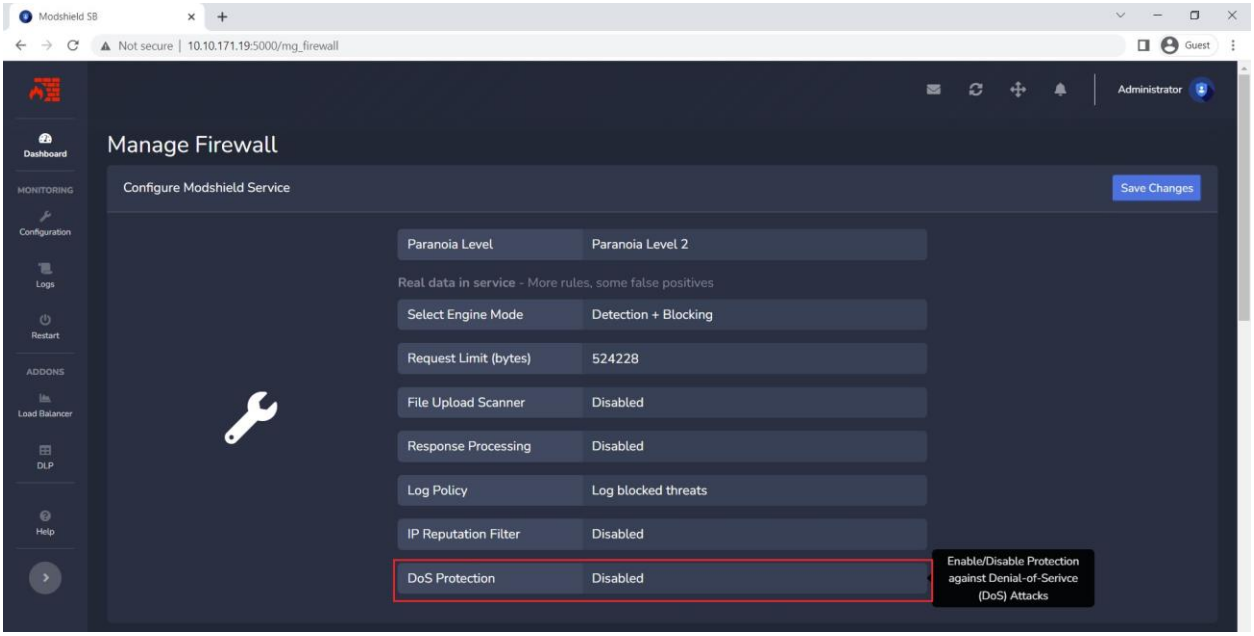


There might be a slight compromise on performance when this filter is enabled

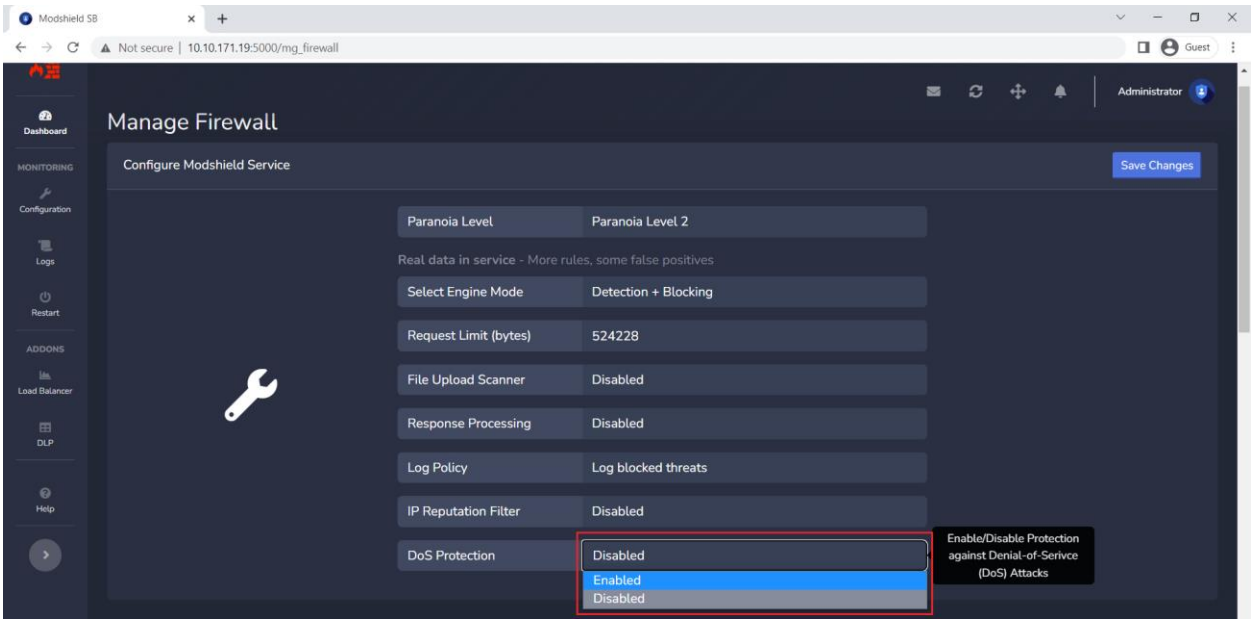
Denial of Service Protection

The next setting that we will talk about is DoS protection

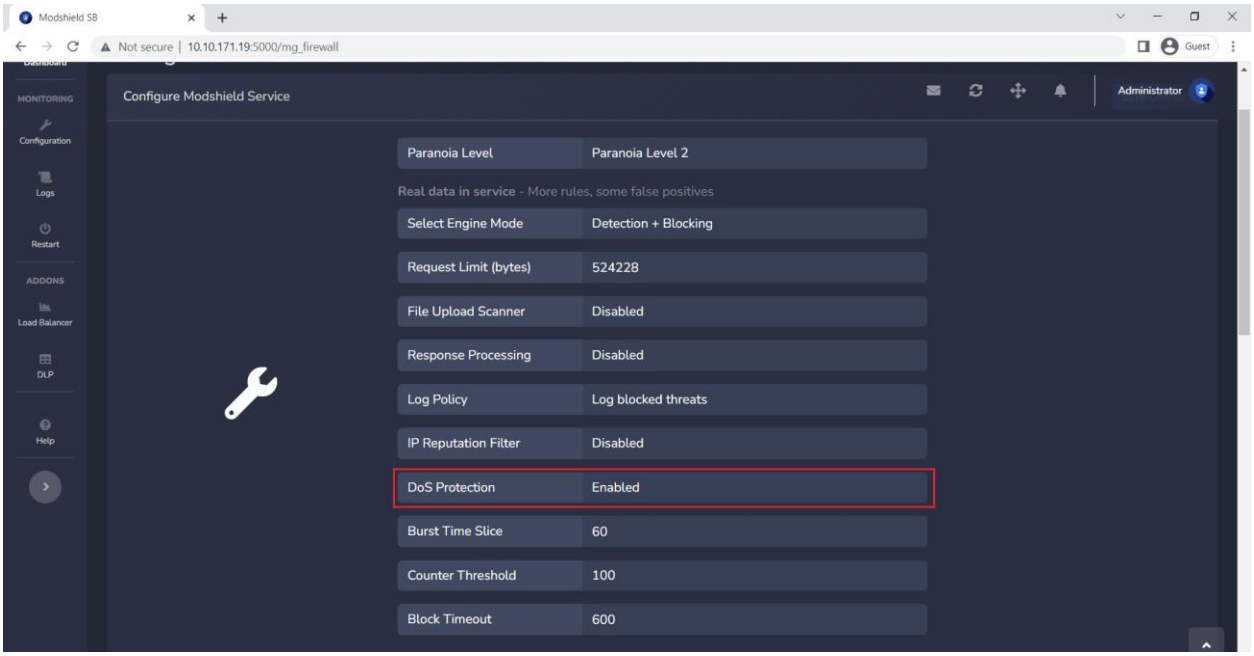
This setting is disabled by default



Enabling this setting will also require you to define the parameters for identification



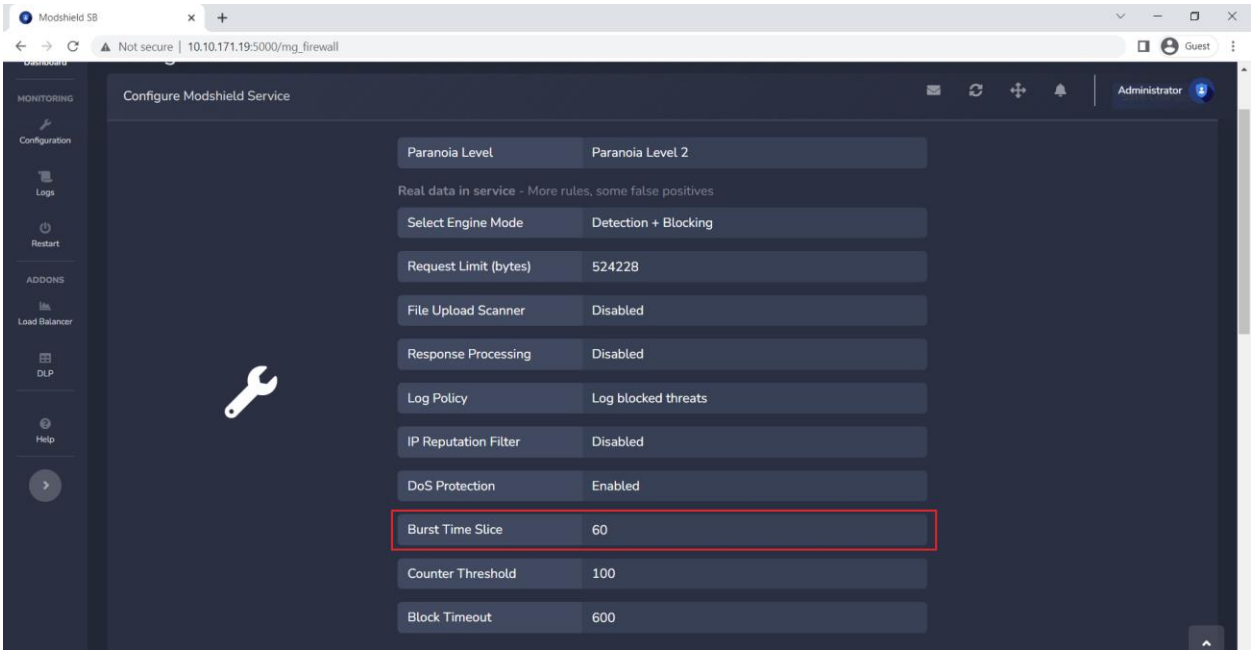
You will have to define these parameters so that a DoS attack can be identified accordingly



For example, 100 requests from an IP, within 60 seconds, can be considered as an attack

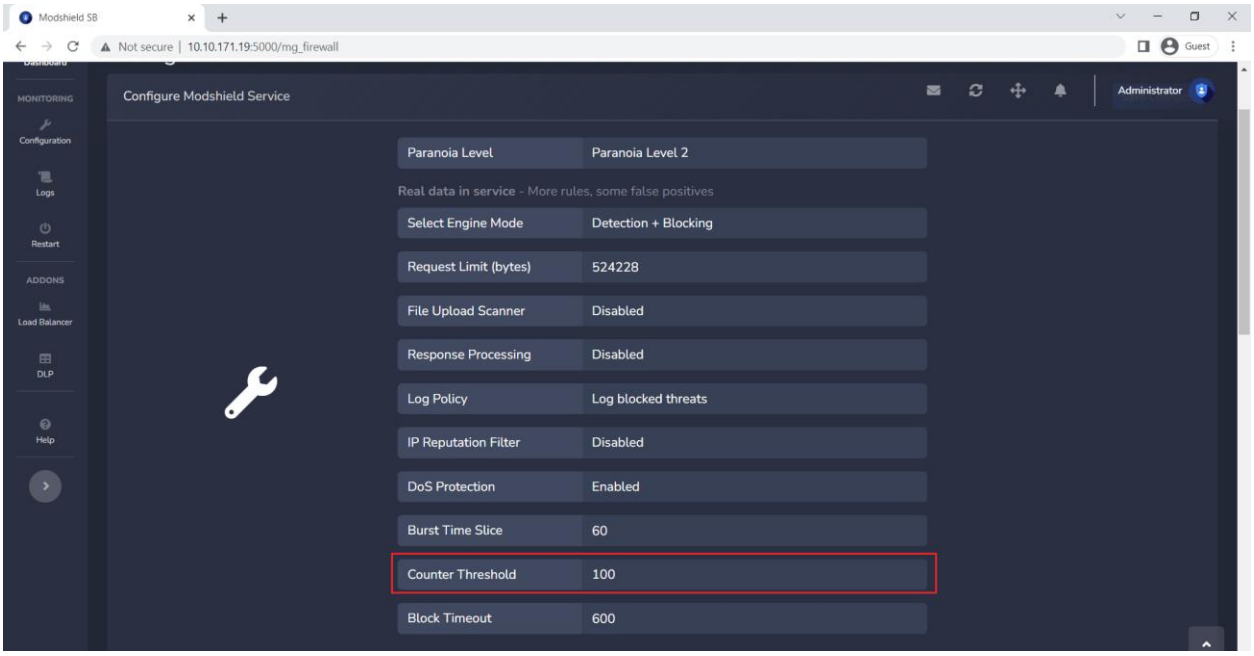
Let's see how we set this in the firewall and block that IP for 600 seconds or 10 minutes

The first setting, **Burst Time slice**, defines the time period for identification



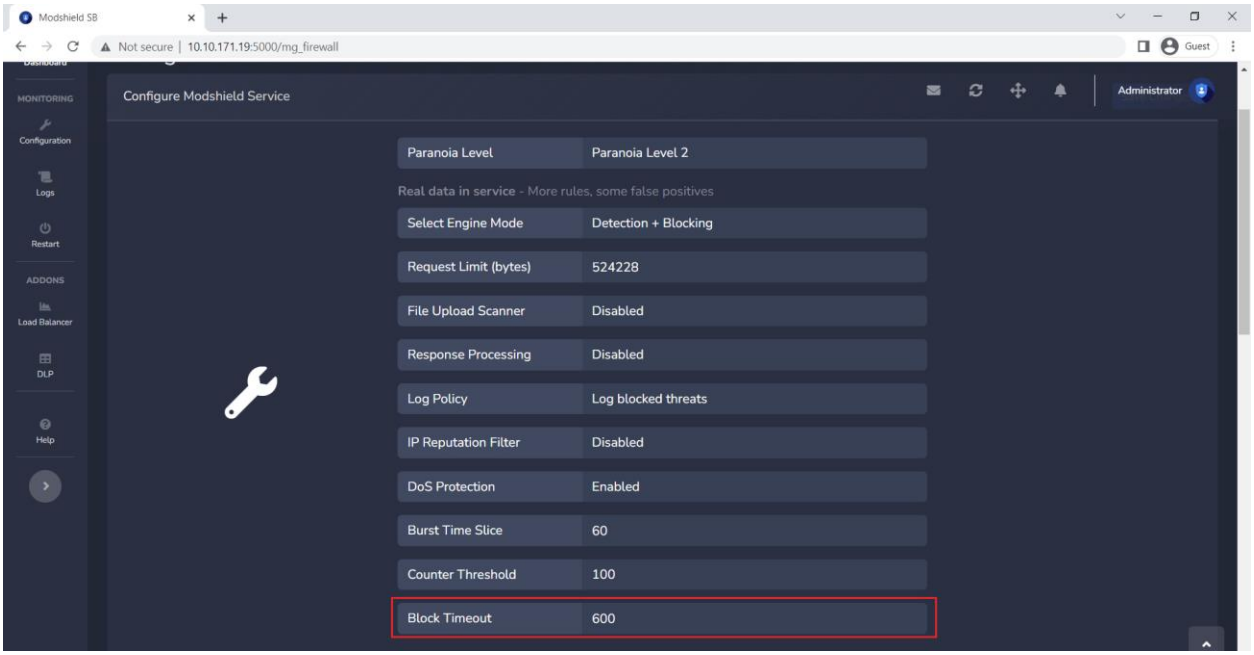
Here, the count of the number of similar requests will be reset every 60 seconds

The **threshold** defines the maximum allowable number of requests within the burst time slice



If there are 100 similar requests within 60 seconds, it is identified as an attack

The IP from which the requests arise is then blocked for the timeout interval

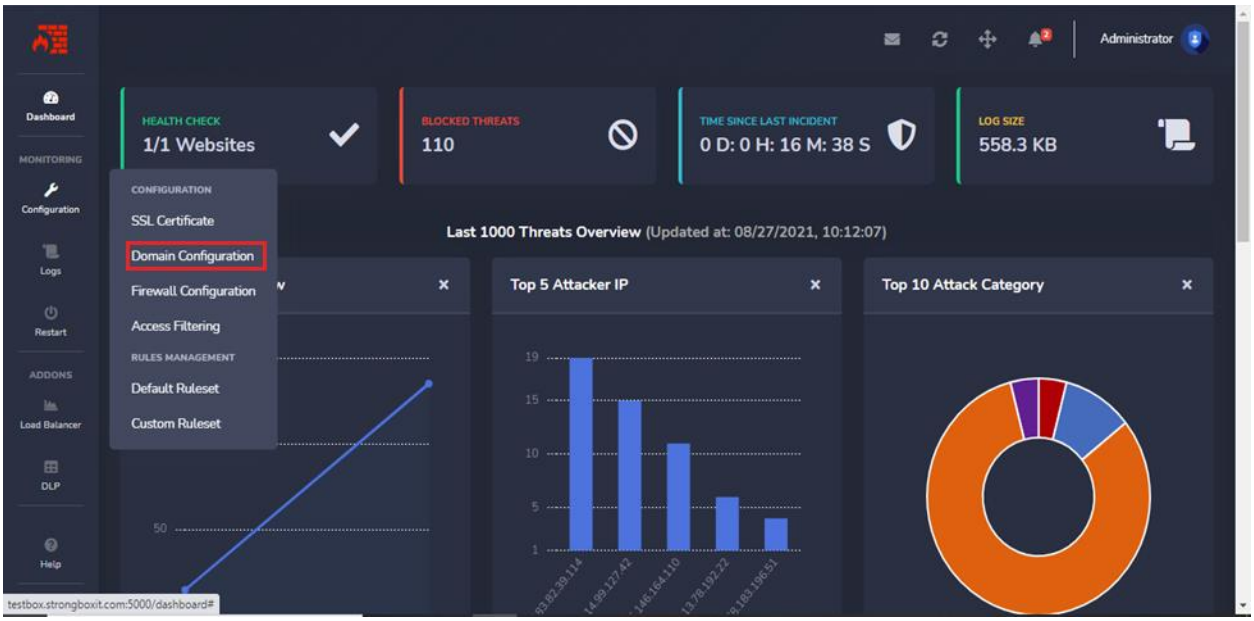


Any IP sending out more than 100 requests within 60 seconds gets blocked for 600 seconds.

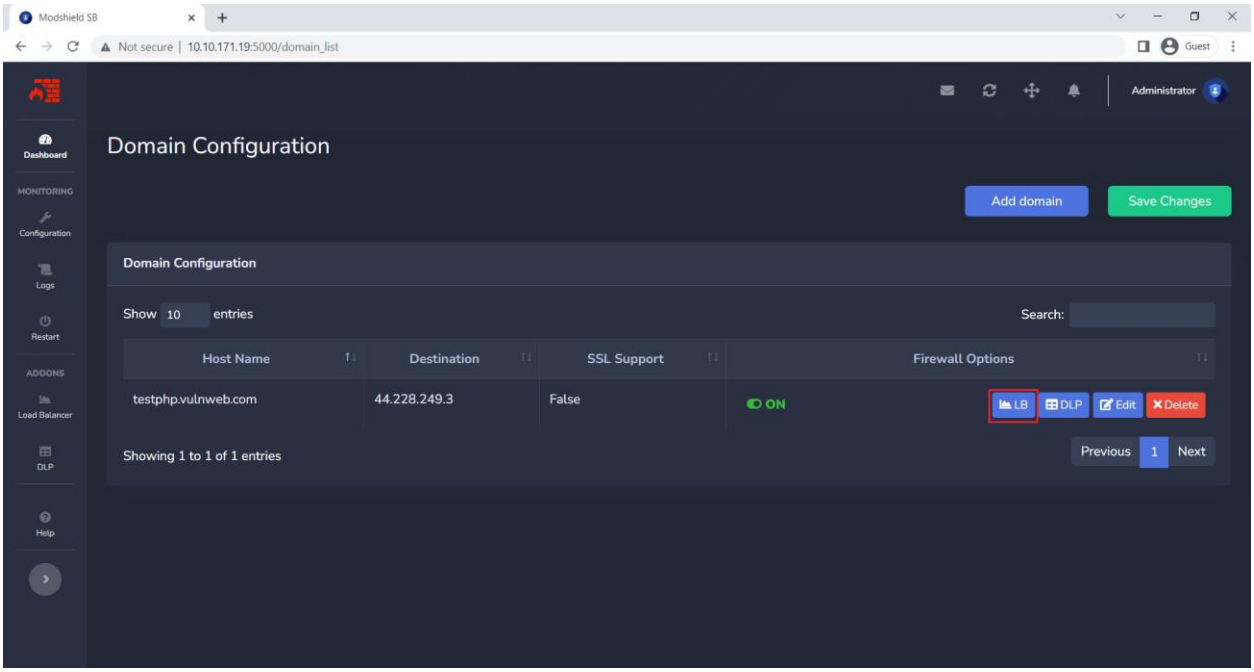
Load Balancer Configuration

Video Link: https://youtu.be/GxNRHpZsaxY

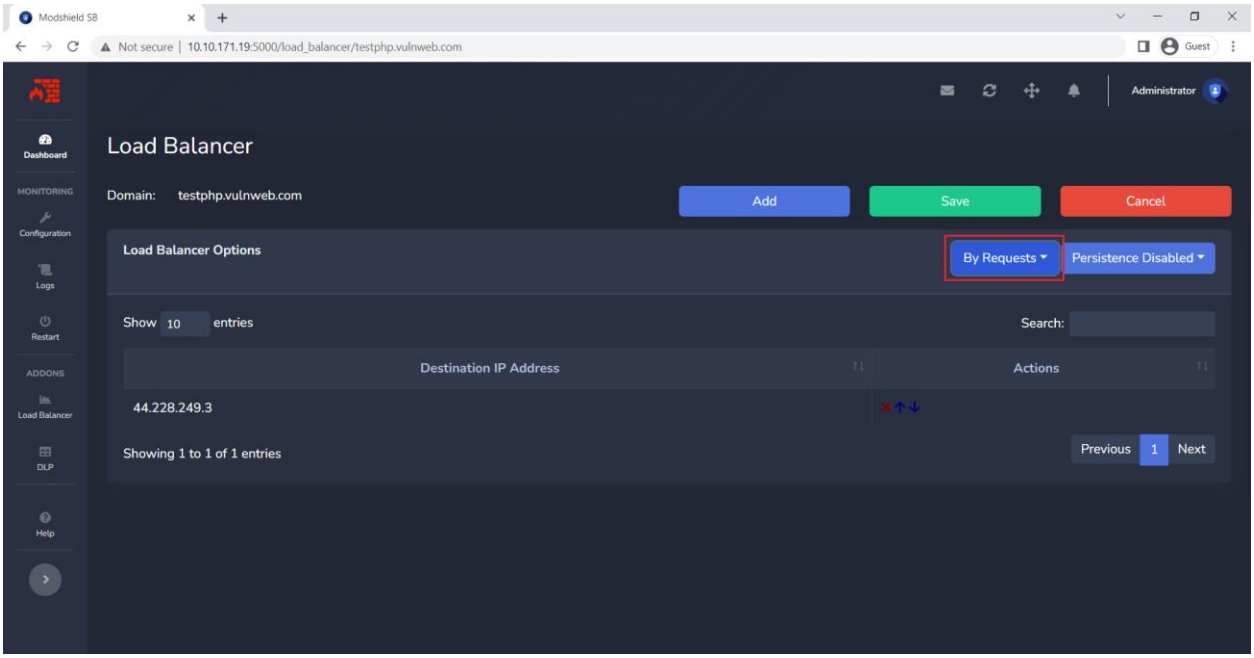
Login to Modshield and select Domain Configuration from the Configuration menu



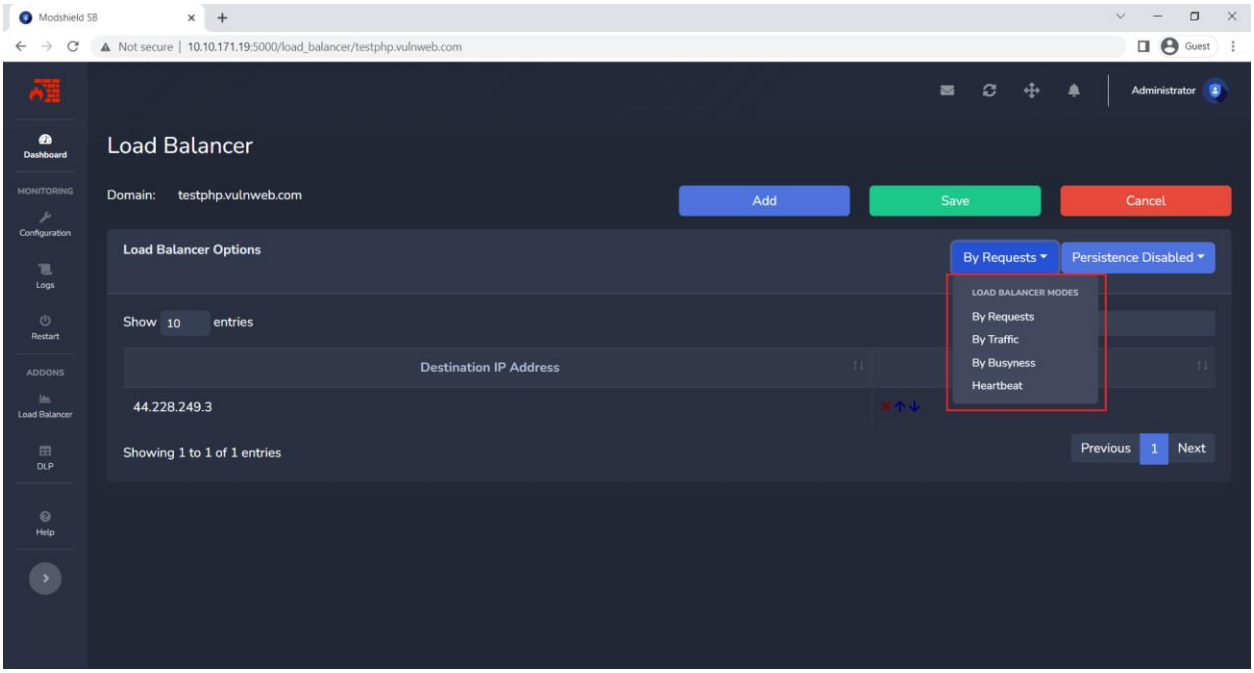
Click on the LB button next to the domain for which you want to configure the load balancer.



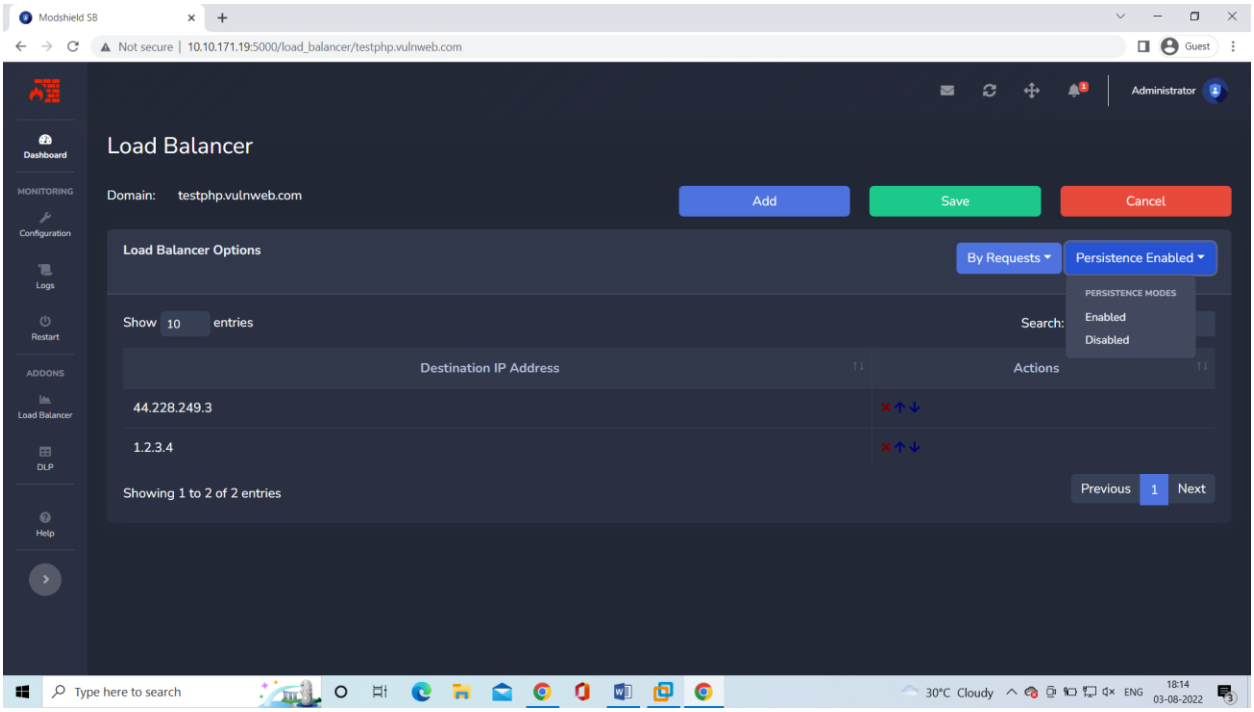
The Load Balancer Options option allows you to set the different modes of load balancing



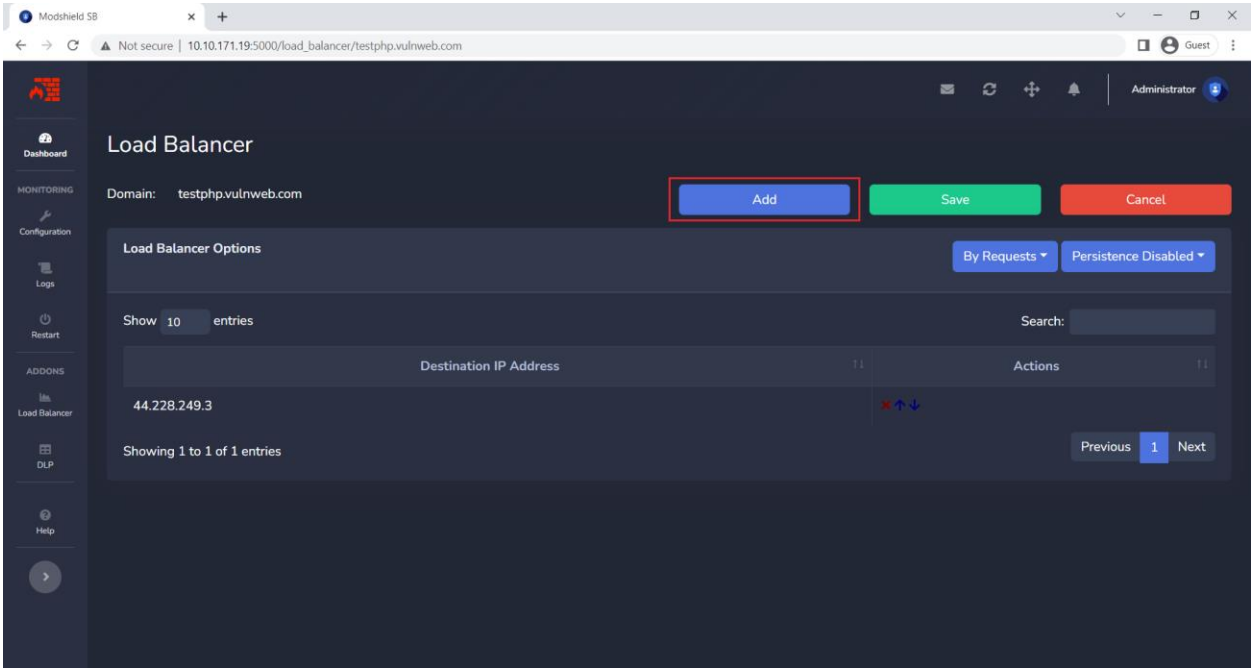
Choose the mode that best suits your requirement



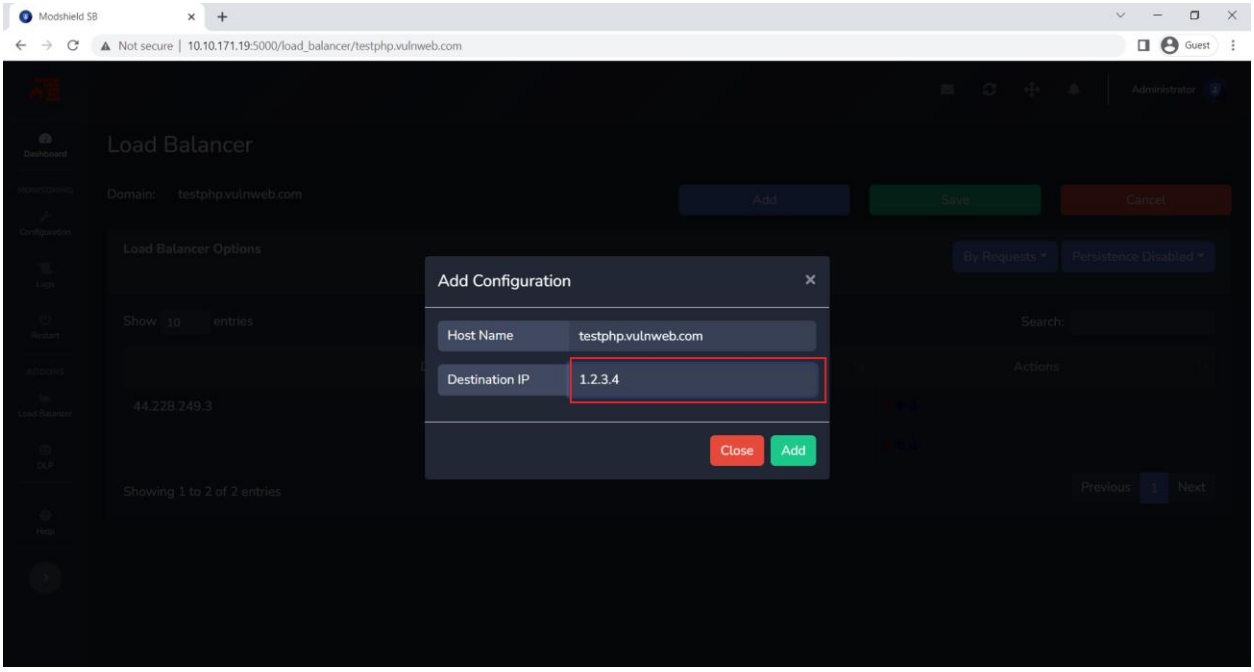
To enable persistence which is disabled by default, simply click on the field and choose enable.



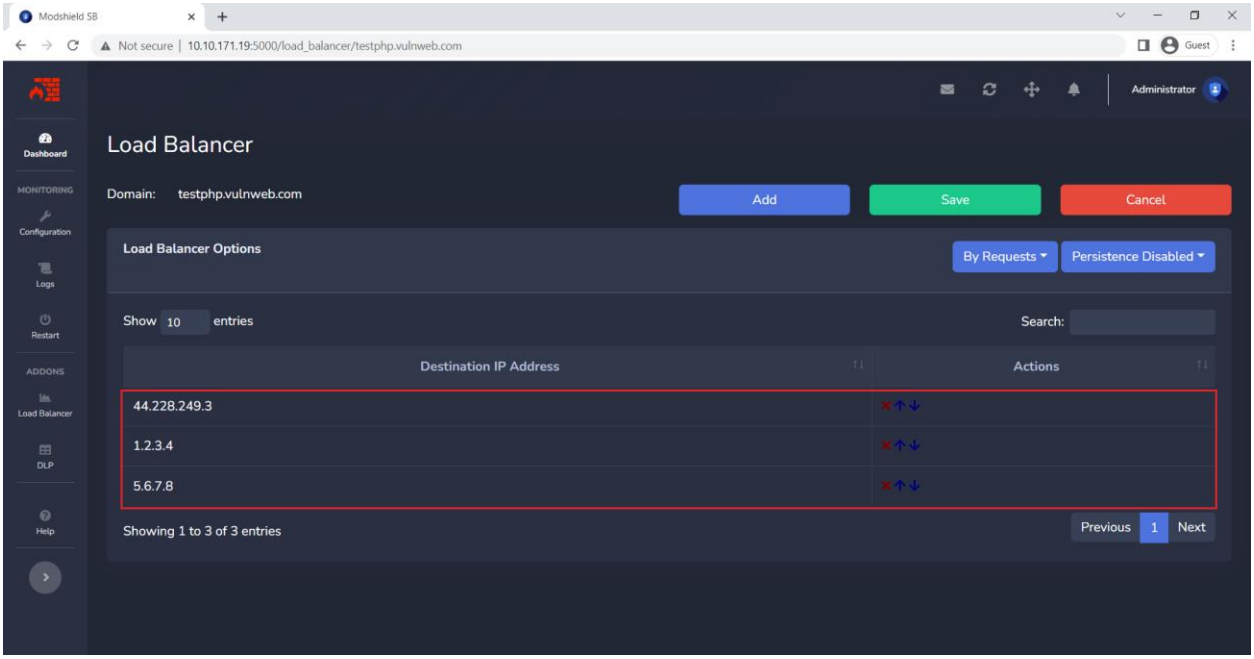
Click on the Add button to add all the IP addresses that host the application



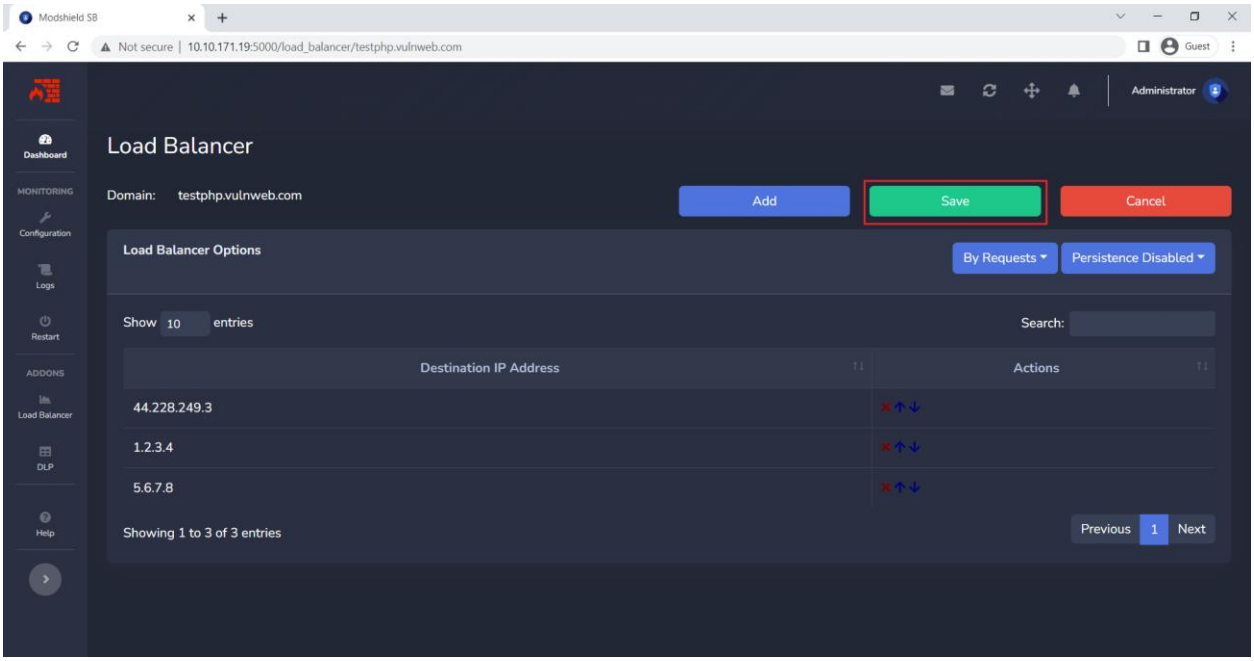
Enter the IP address in the destination IP field and click on Add



This adds the IP address to the list of servers the application is hosted on

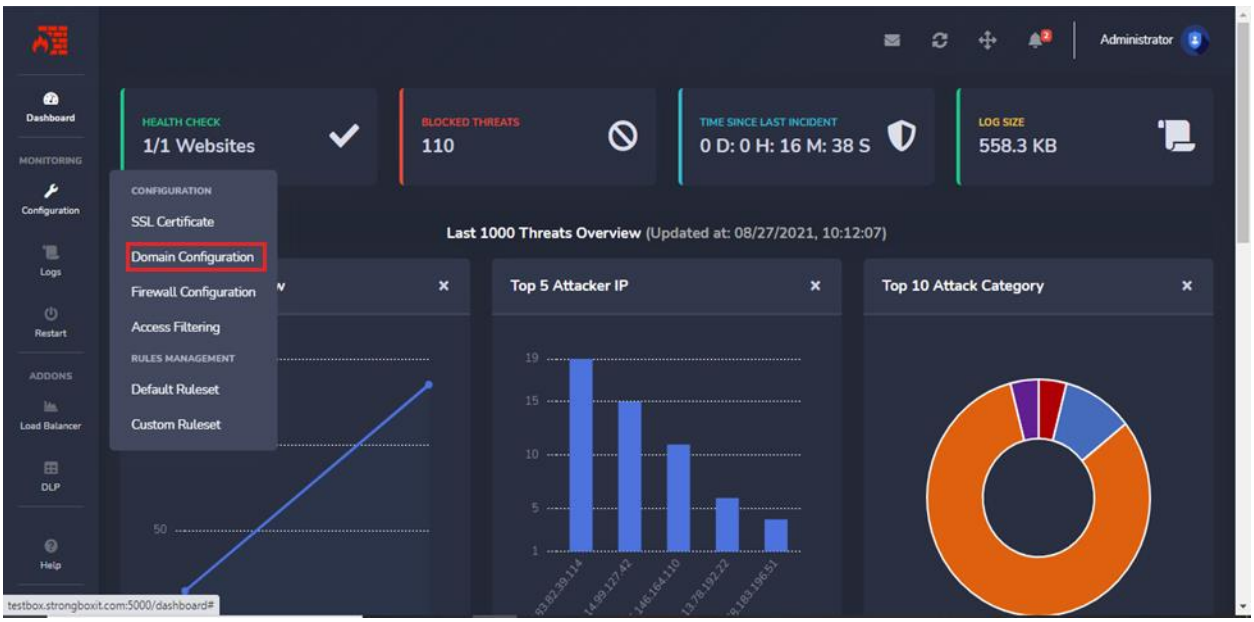


Repeat this for all the IP addresses that you wish to add and then click on Save

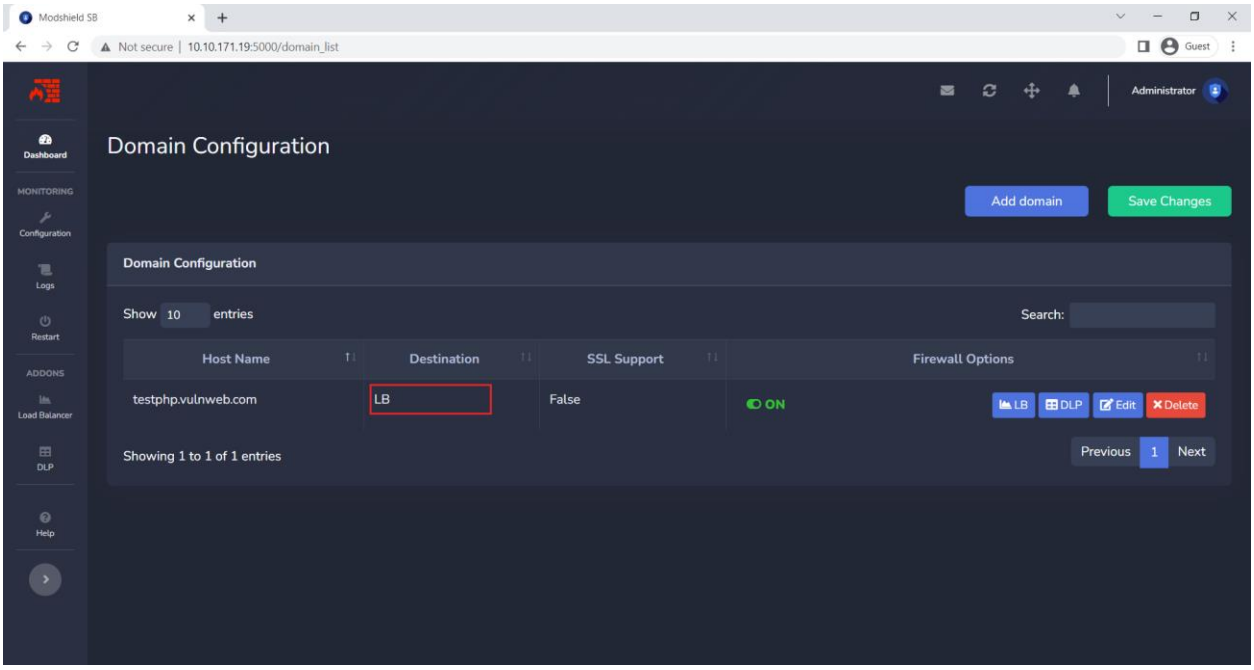


You have now successfully configured the load balancer

To Verify the change, Open the Domain Configuration from the configuration menu



Notice that the destination for the domain has been changed to LB instead of a single IP address

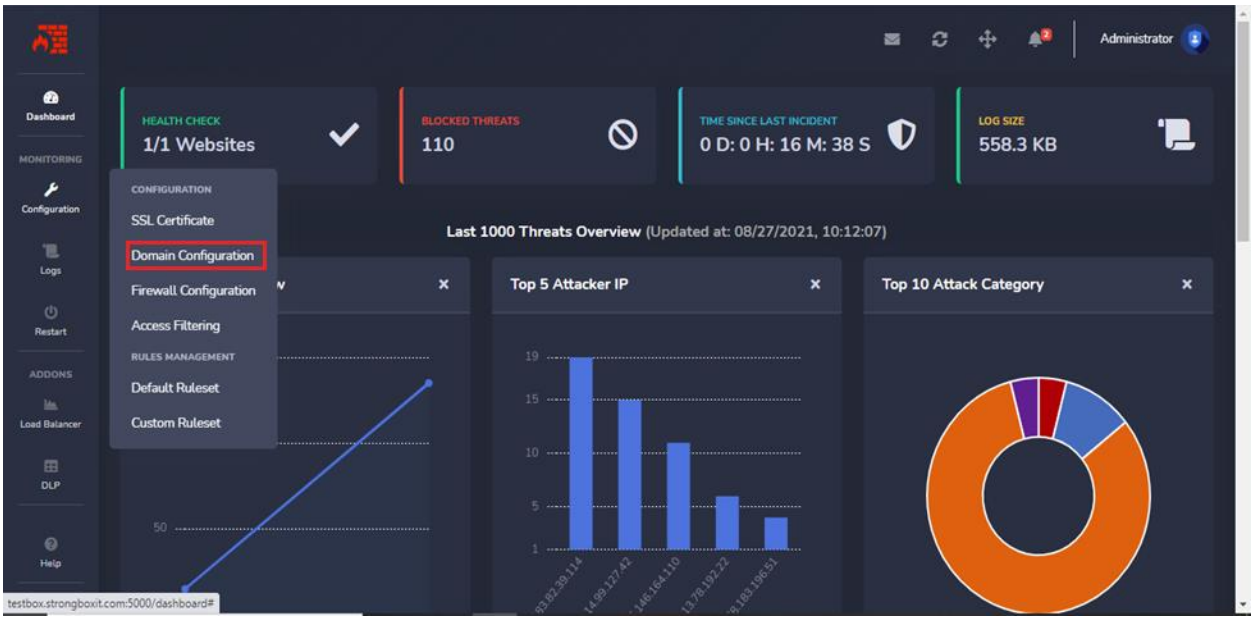


You can also do this from the Load Balancer menu. Simply choose the domain from the menu and configure as shown earlier. Do not forget to Save your changes

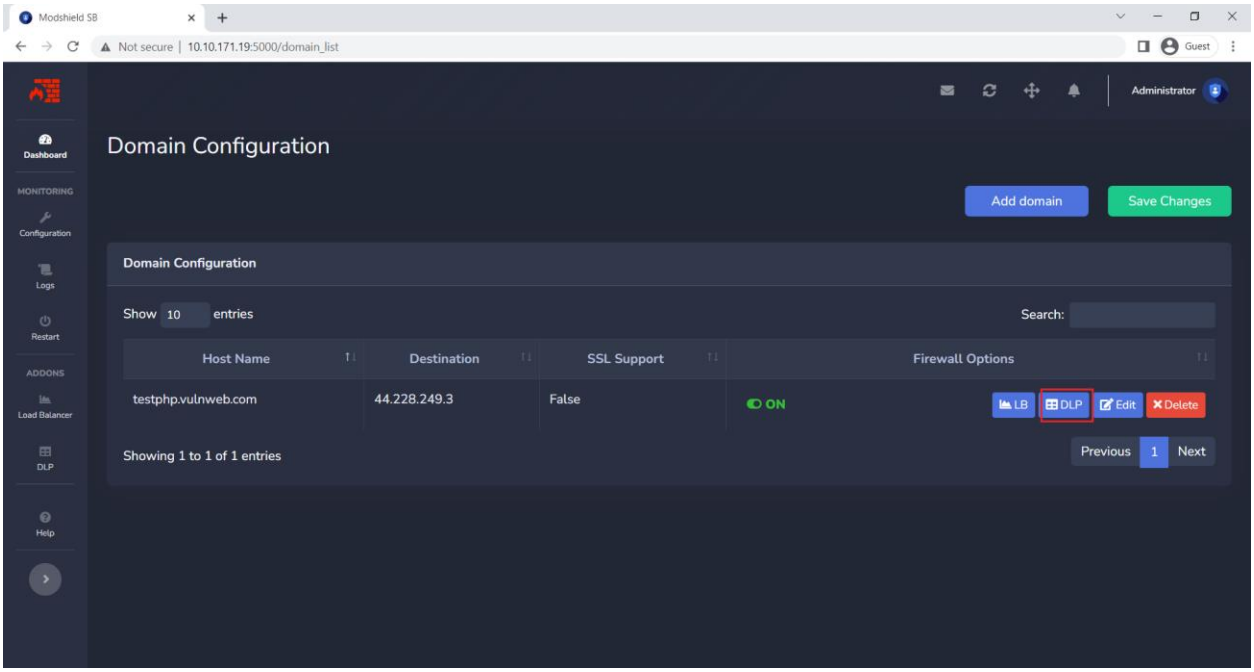
Data Loss Prevention

Video Link: https://youtu.be/GxNRHpZsaxY

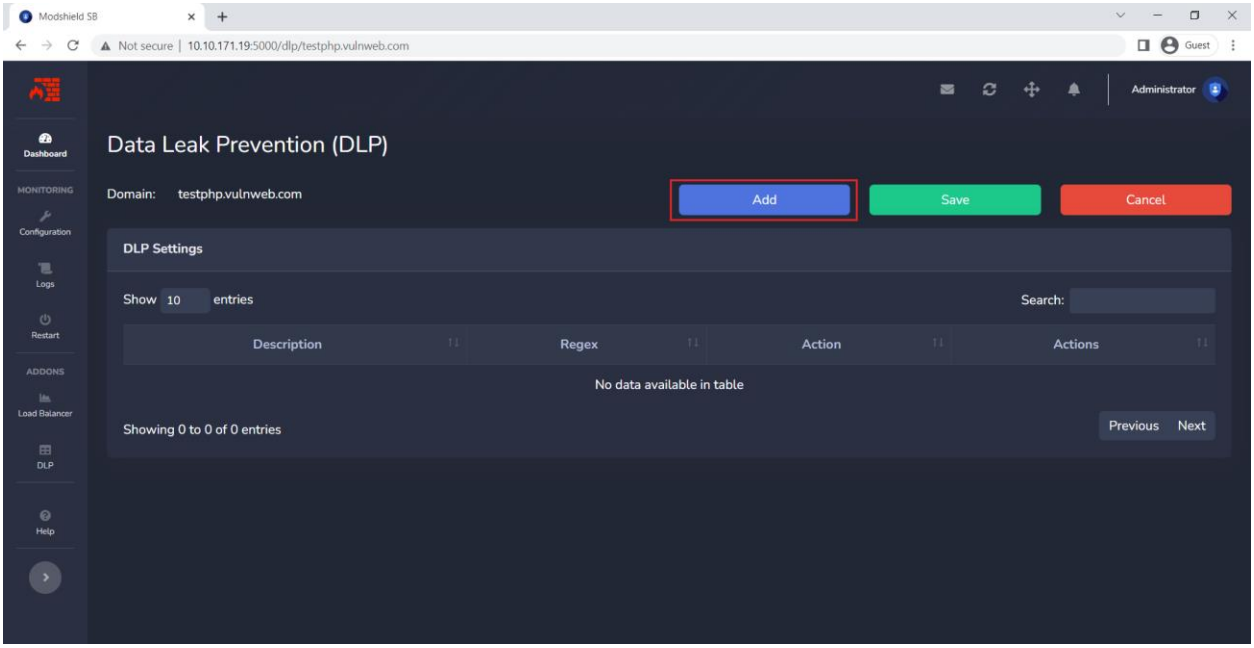
To Configure Data Loss Prevention, Open the domain configuration from the configuration menu



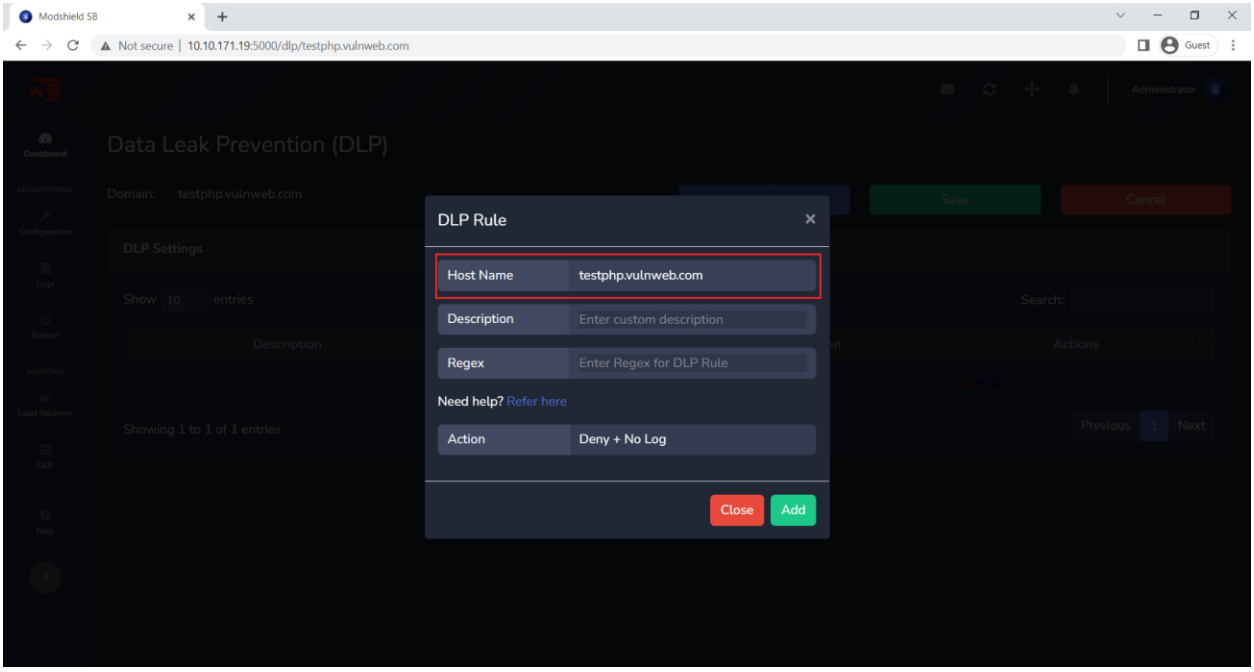
Click on the DLP button next to the domain for which you would like to configure the DLP



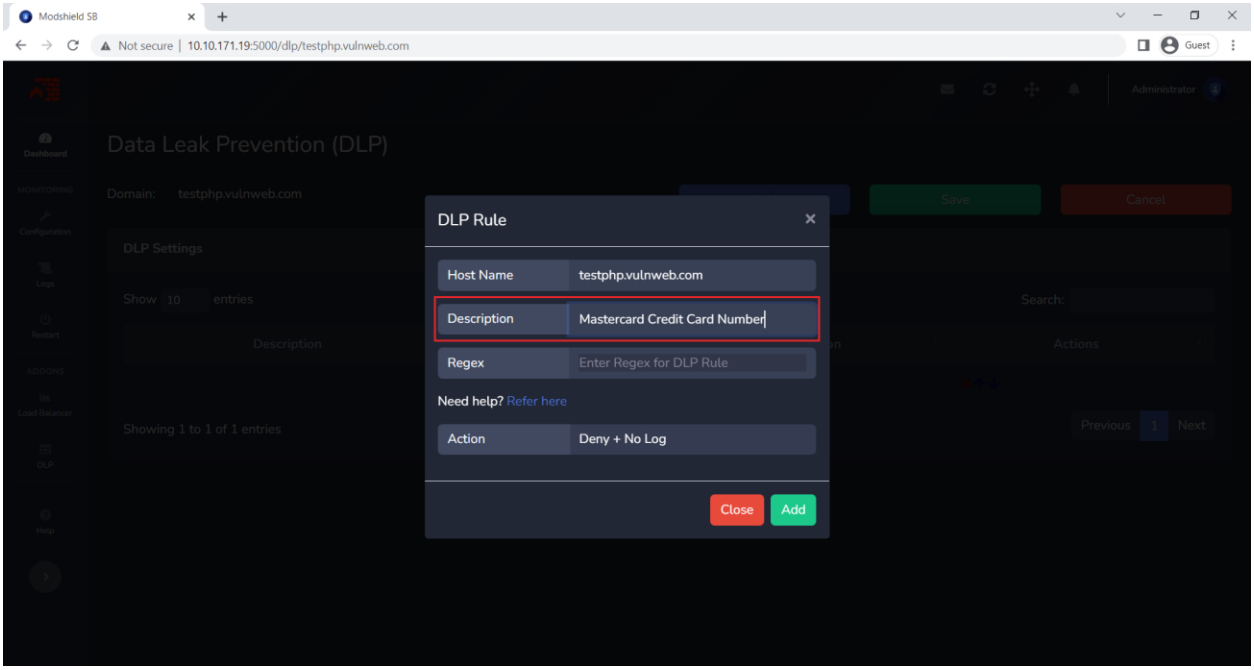
Click on Add to instruct Modshield on the format of data that is considered as sensitive



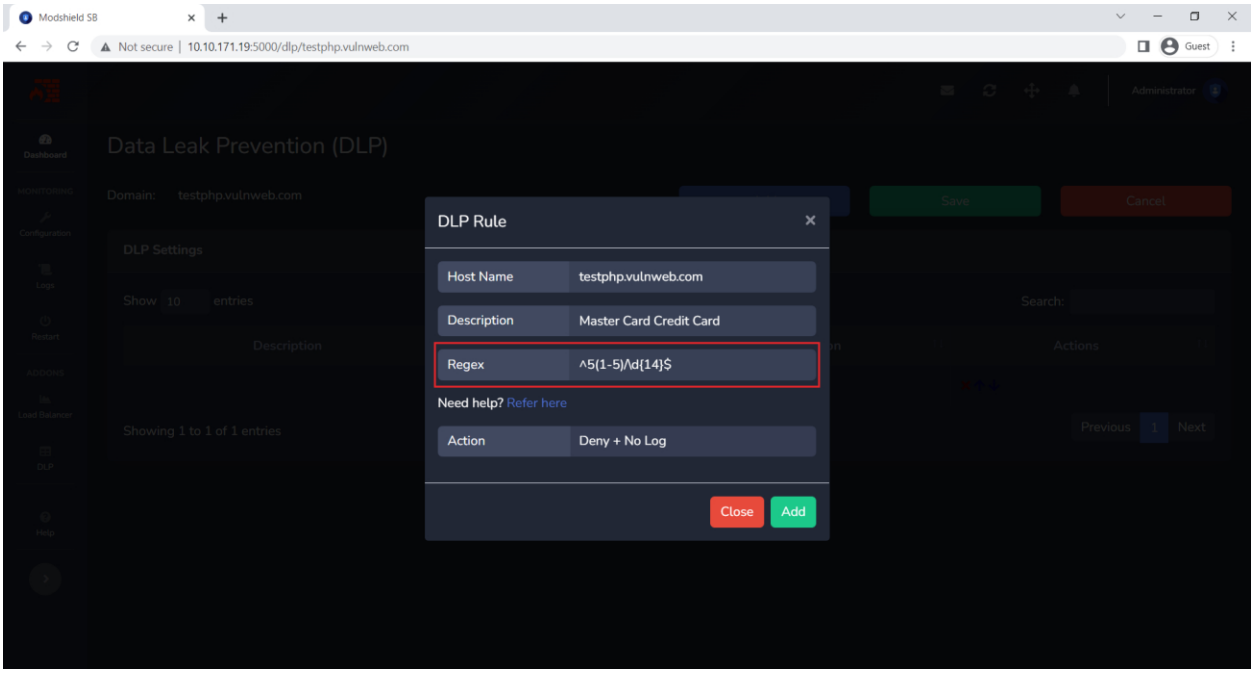
Enter a name for your rule to easily identify what this data pattern is for...



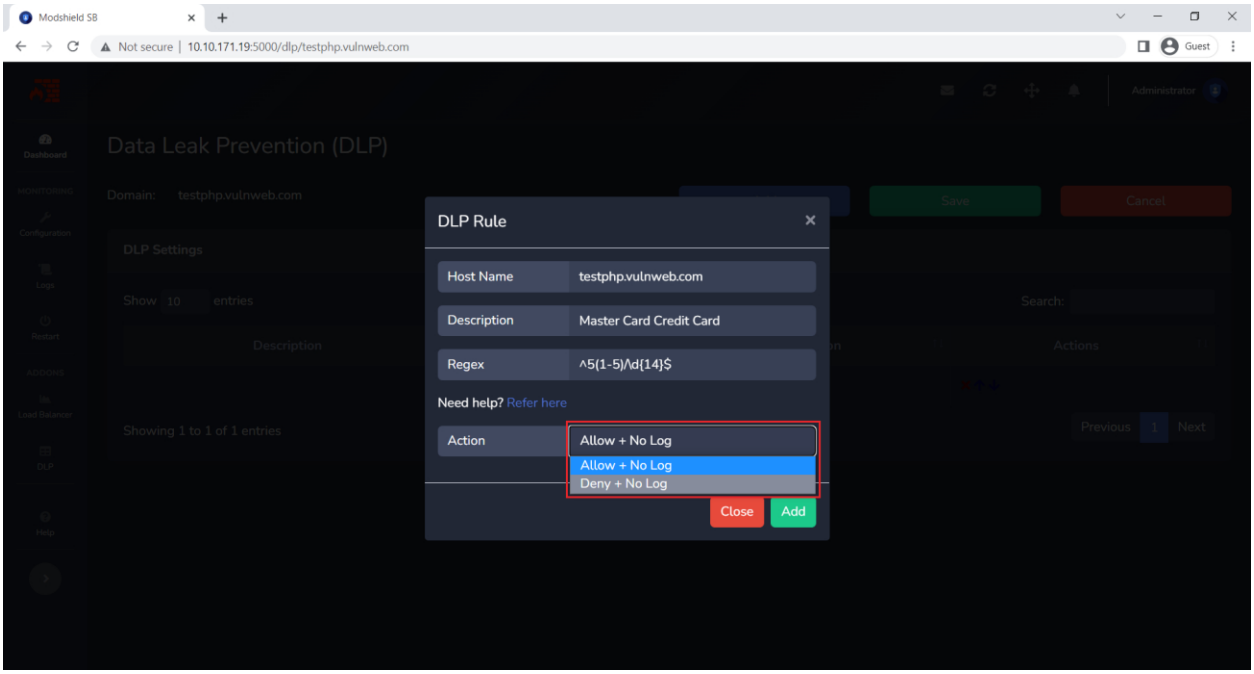
I am going to restrict all responses that have a master card number



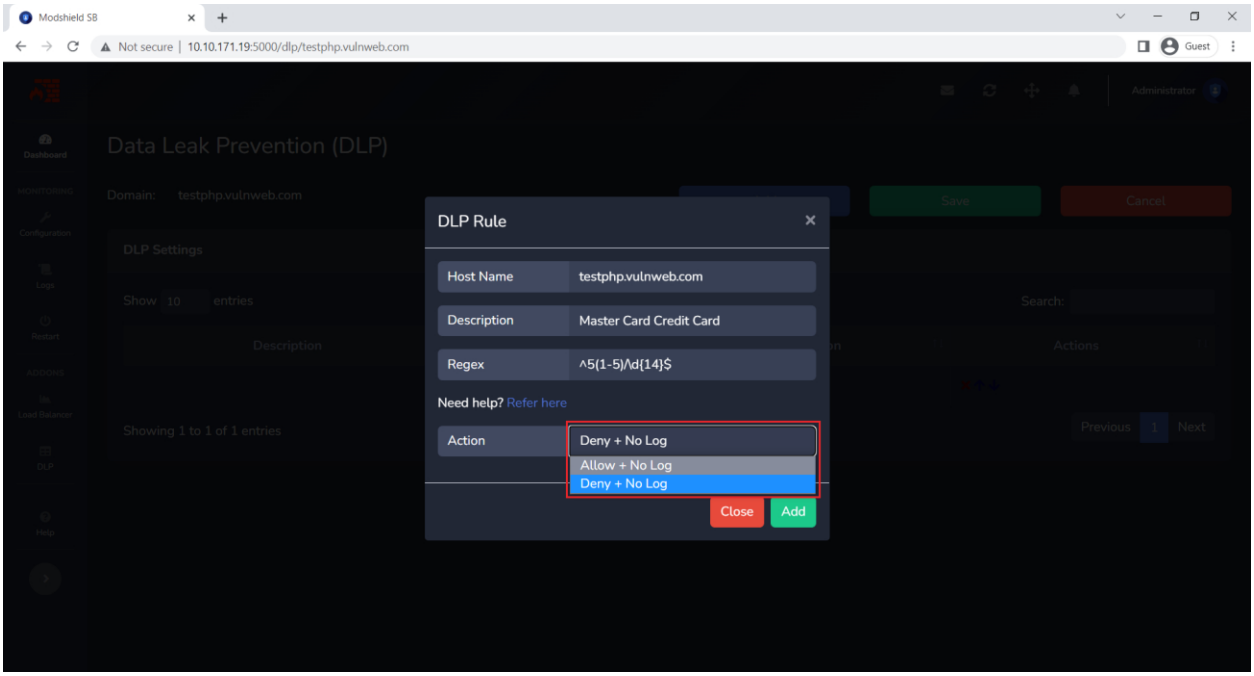
Provide the regex for the data format. Please ensure that the regex is accurate. All responses from the application that contains Mastercard numbers will be filtered



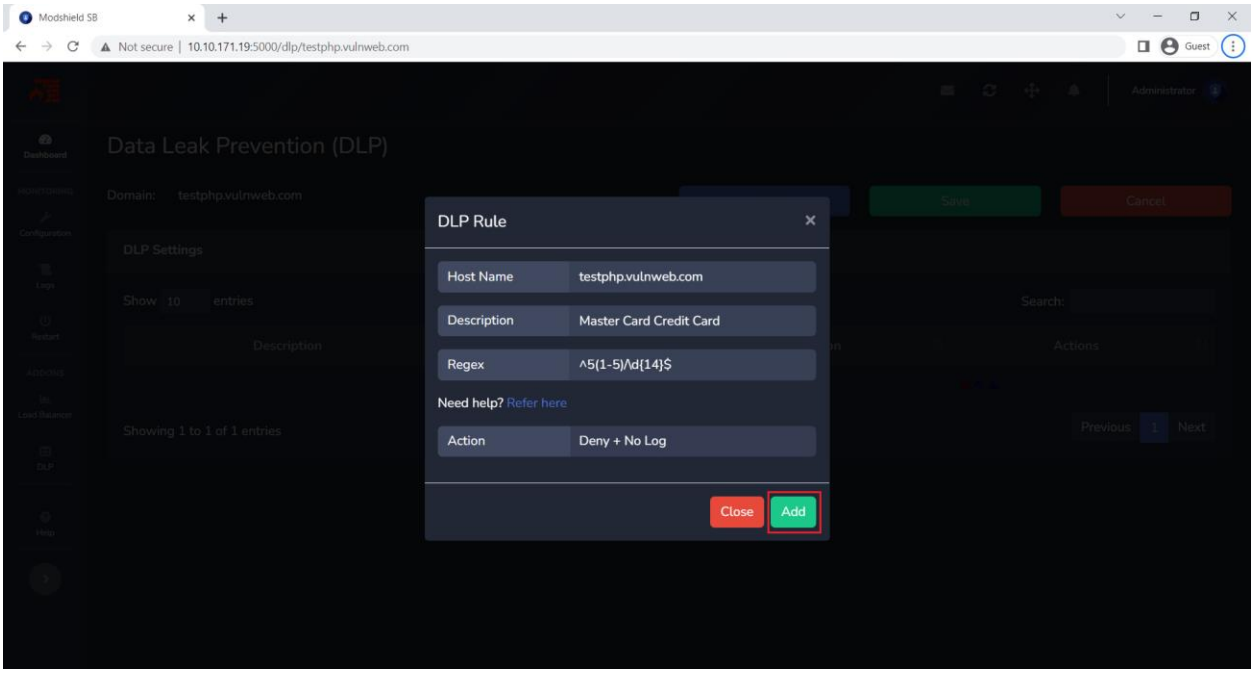
You can choose to allow the response and not store sensitive information in the log files or you can choose to block the response itself. In both cases this data will not be logged



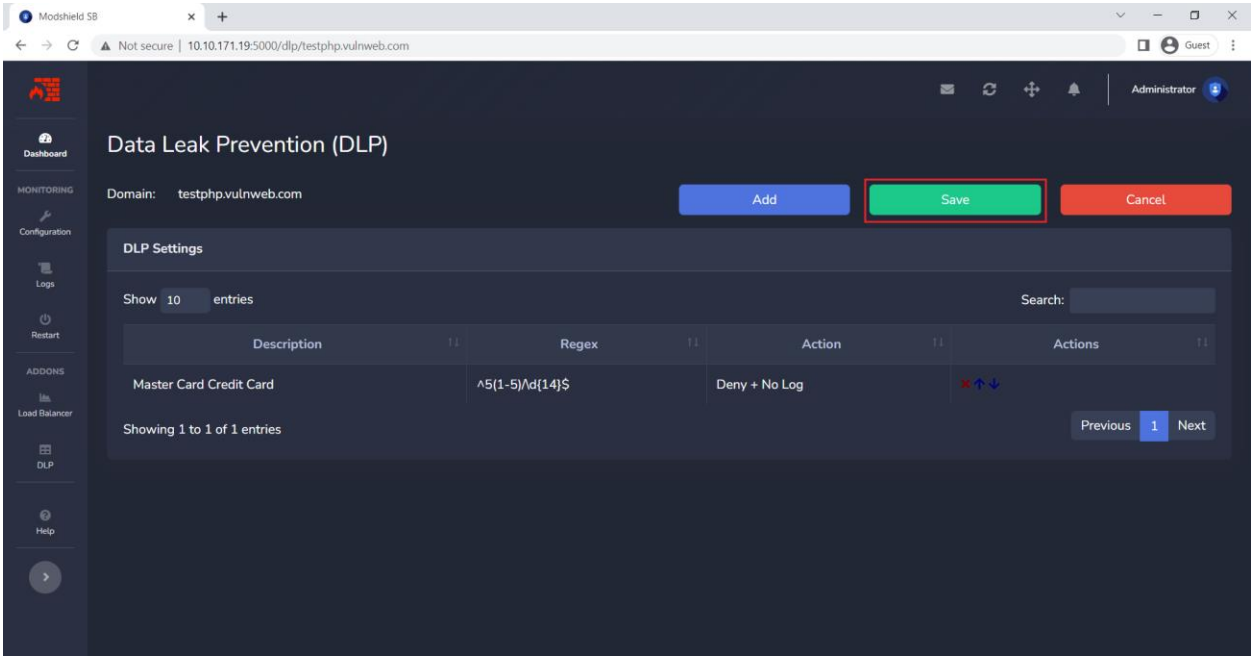
I choose the block all responses with sensitive data



Click on Add to add this condition. You can repeat this to add any number of filters for DLP

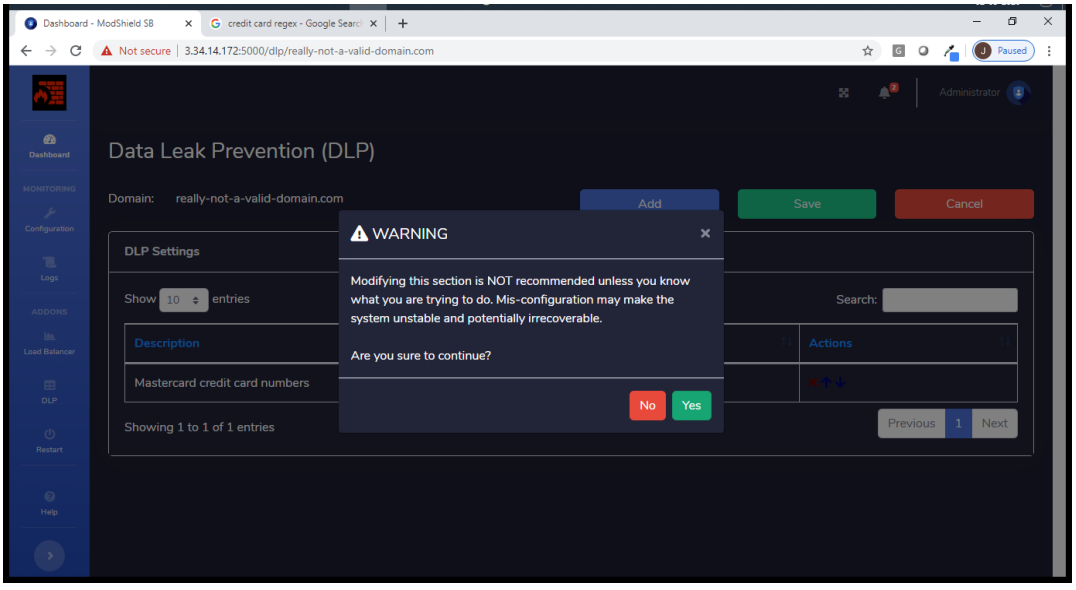


Click on Save to save this change



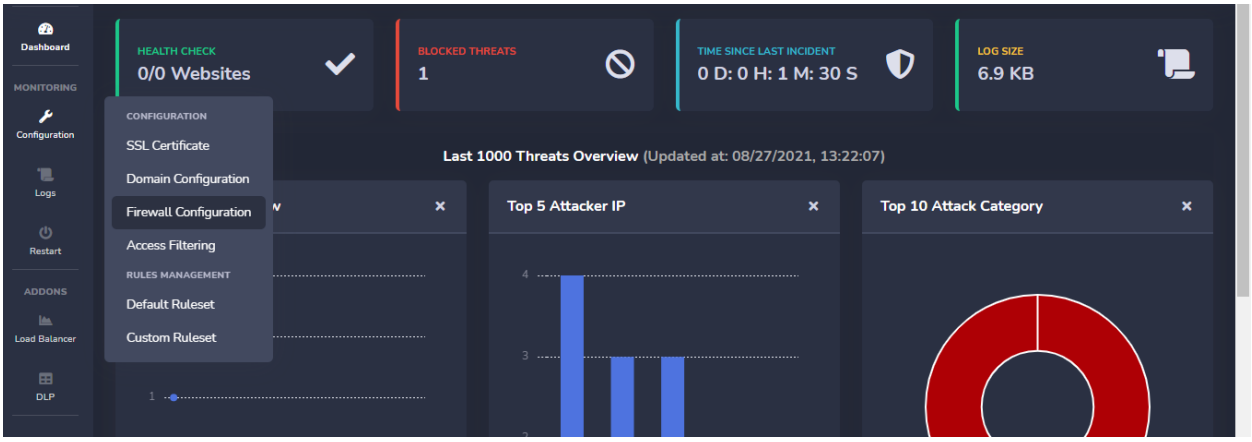
Erroneous Regex might block responses that are safe. Please ensure accuracy of the regex used.

You can also set the DLP rules using the DLP option in the left menu.

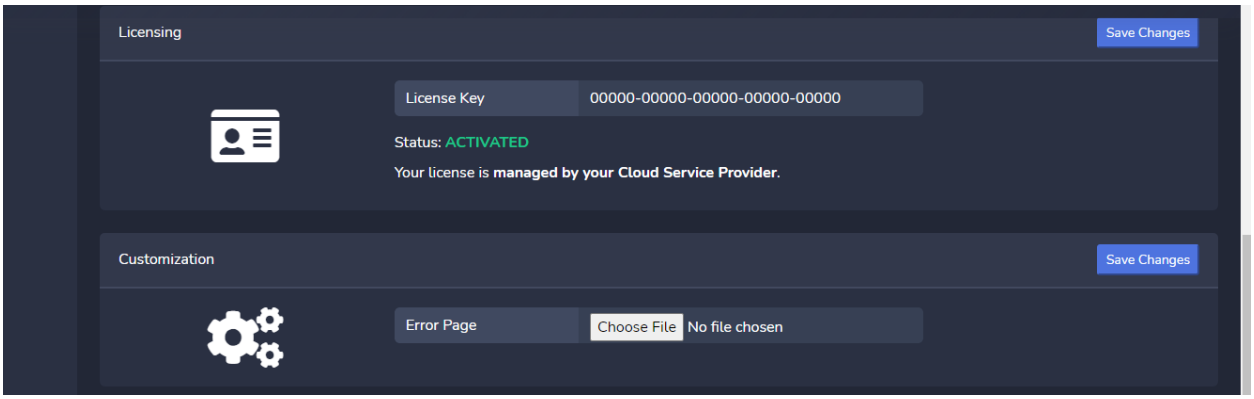


Adding your own error page

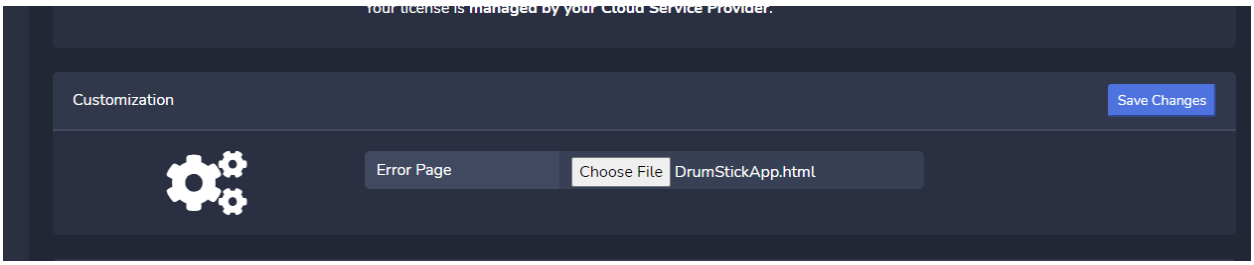
Step 1: To add a custom error page click on configuration ->firewall configuration



Step 2: click on choose file from the customization menu



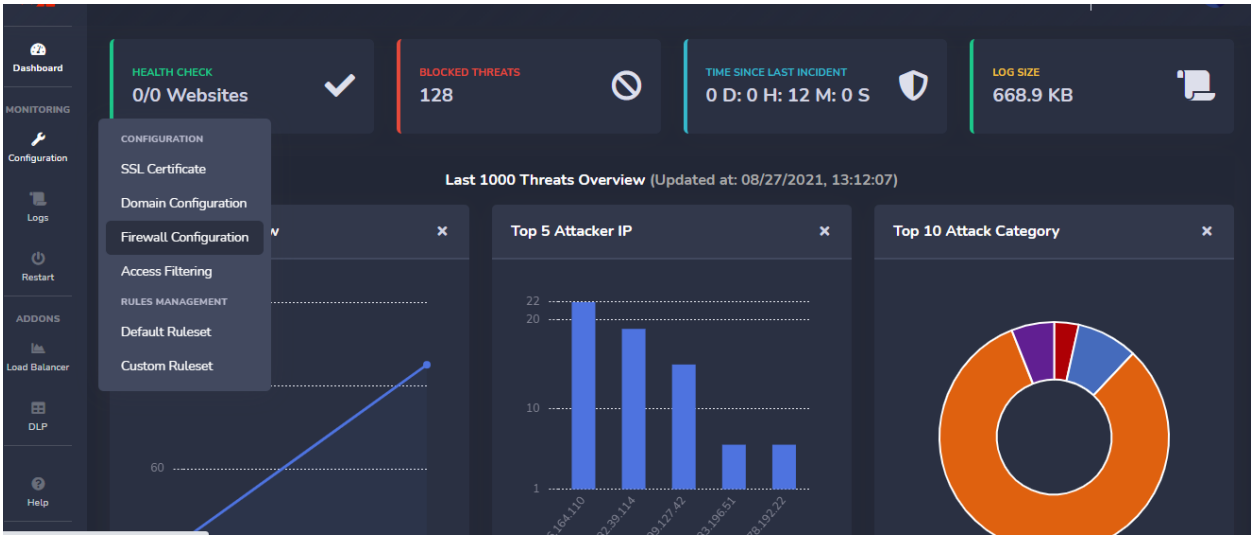
Step 3: You can choose your pre-designed custom error page and upload it. Click on save changes and your custom error page will now be shown every time a request is blocked by Modshield SB



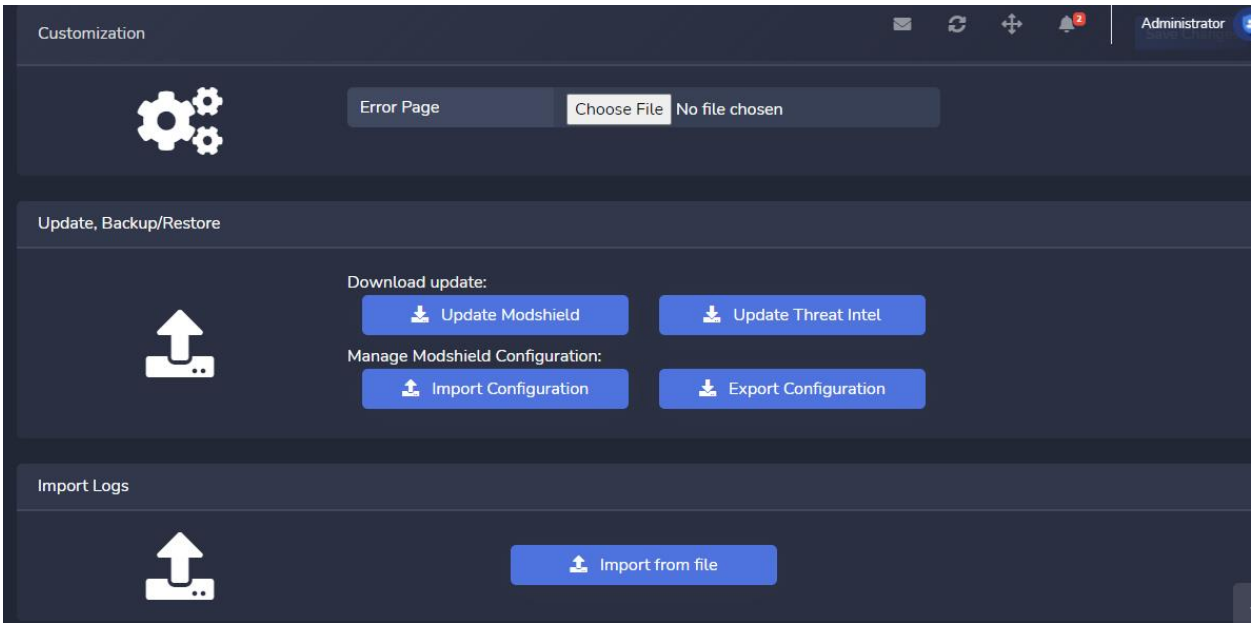
Import Logs

If you migrating between two instances of Modshield SB and would like to import the logs from the first instance to the second, please follow the below steps.

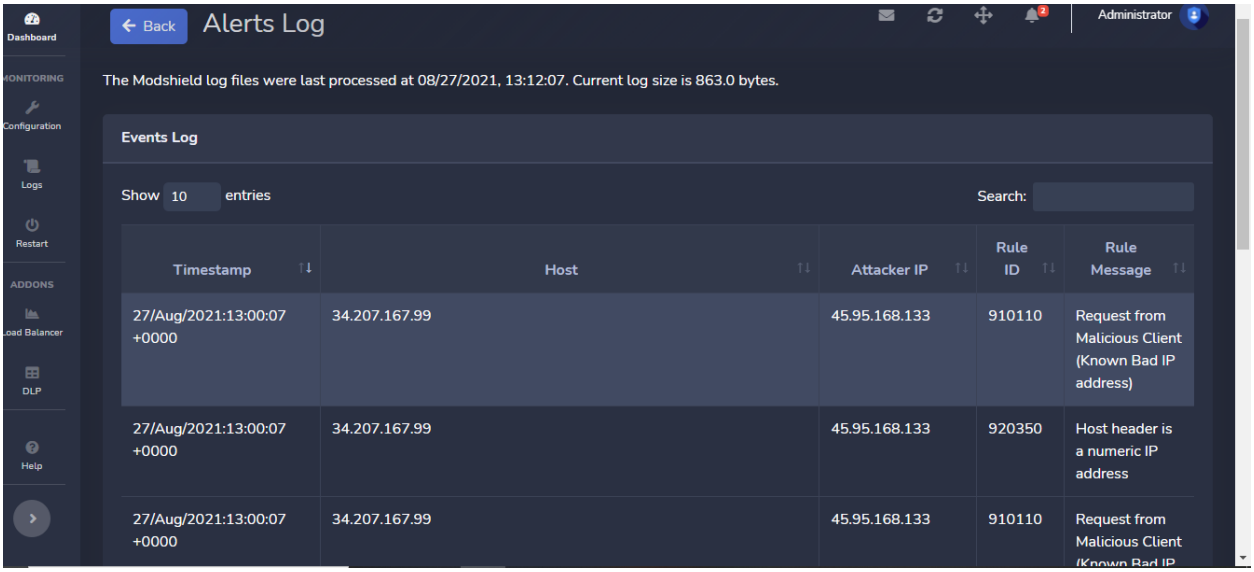
STEP 1: To import logs click on configuration-> firewall configuration



STEP 2: In the firewall configuration page click on import from file in the import log section



STEP 3: Once you have imported the logs it is being processed and can be viewed in the log section

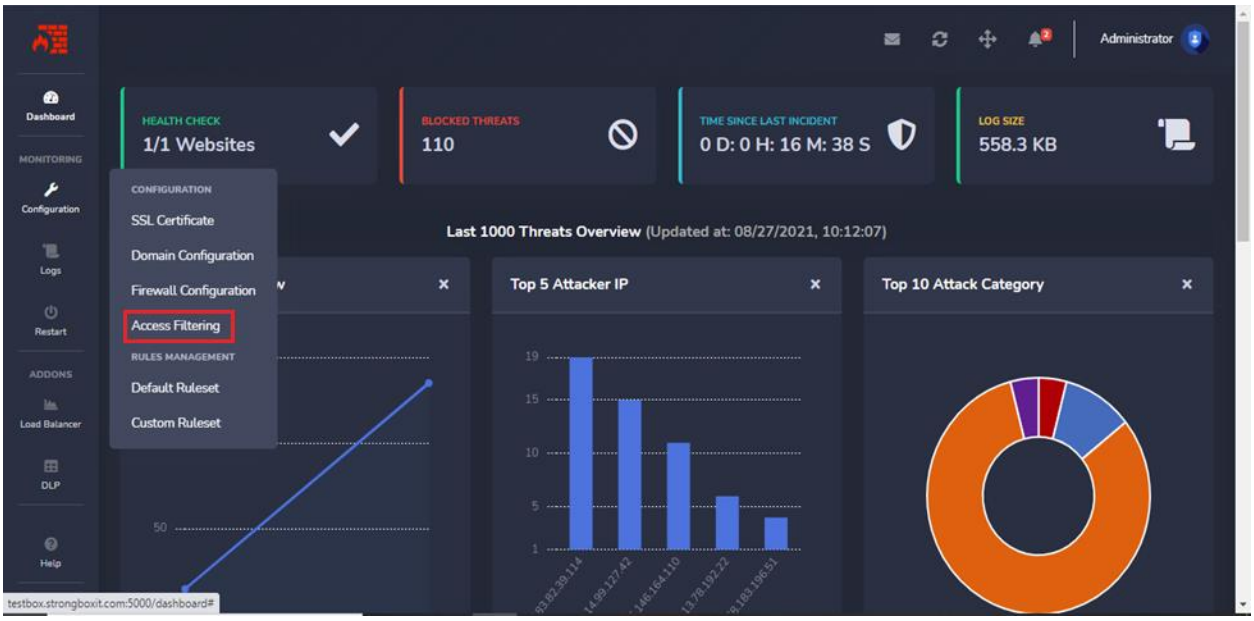


Access Control

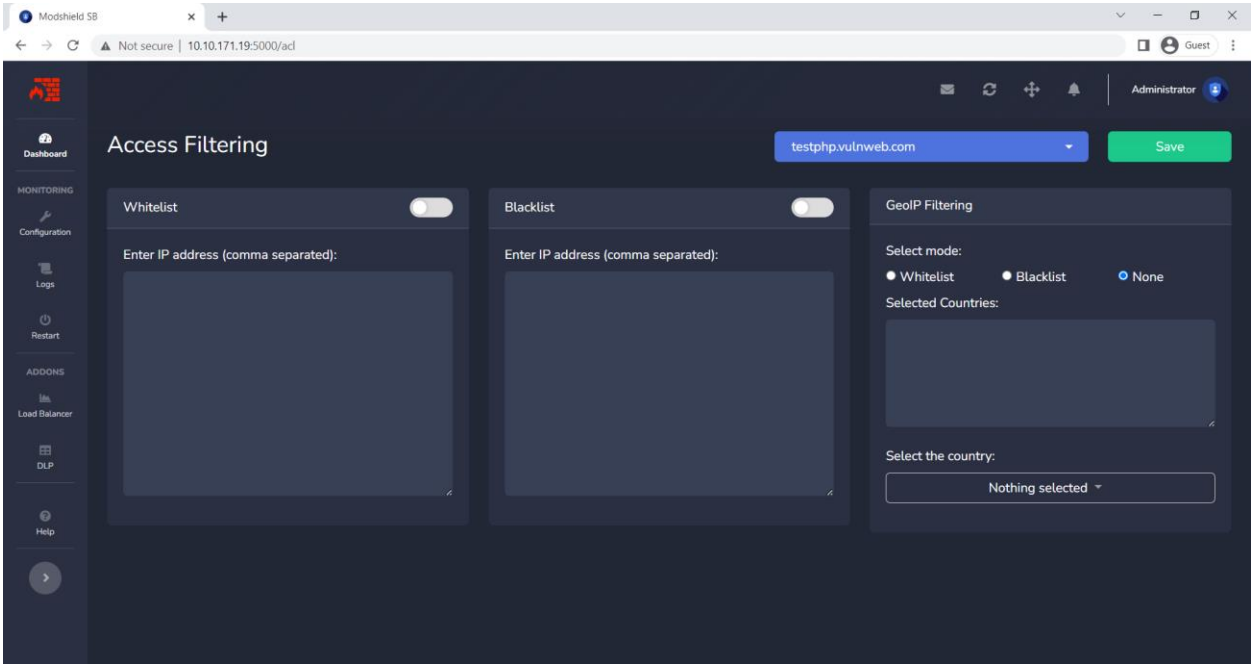
Video Link: https://youtu.be/281NONeWLrg

Whitelists and Blacklists

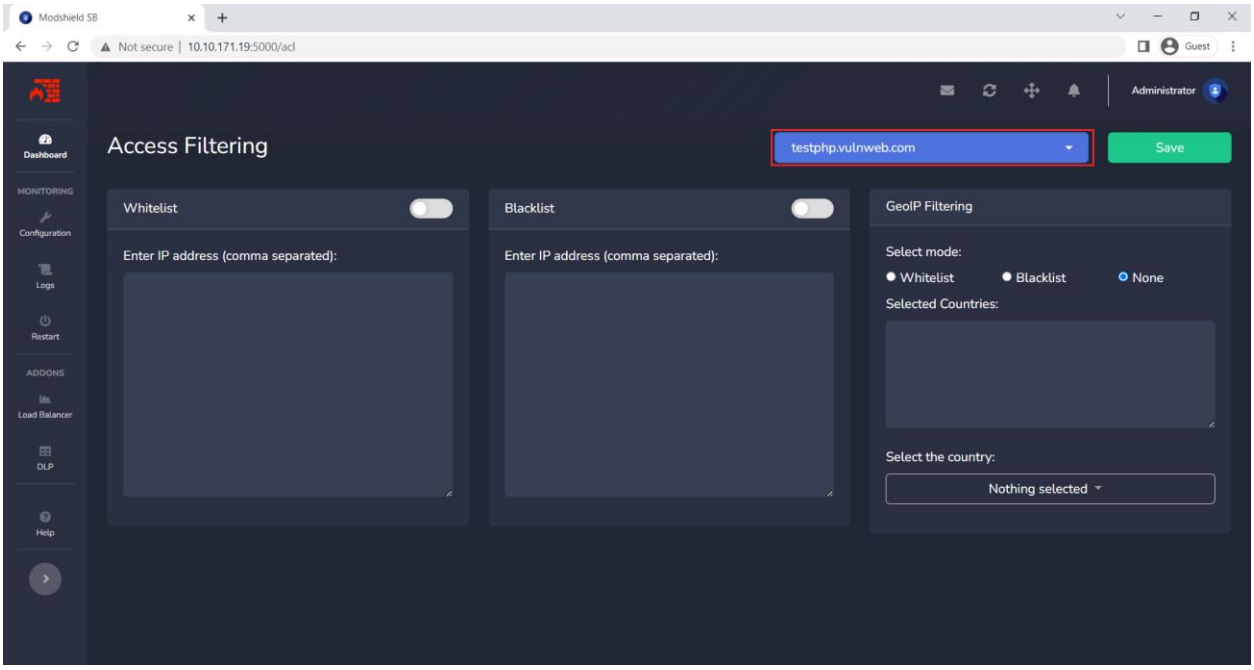
Access filtering allows us to set conditional access to a website or a web application



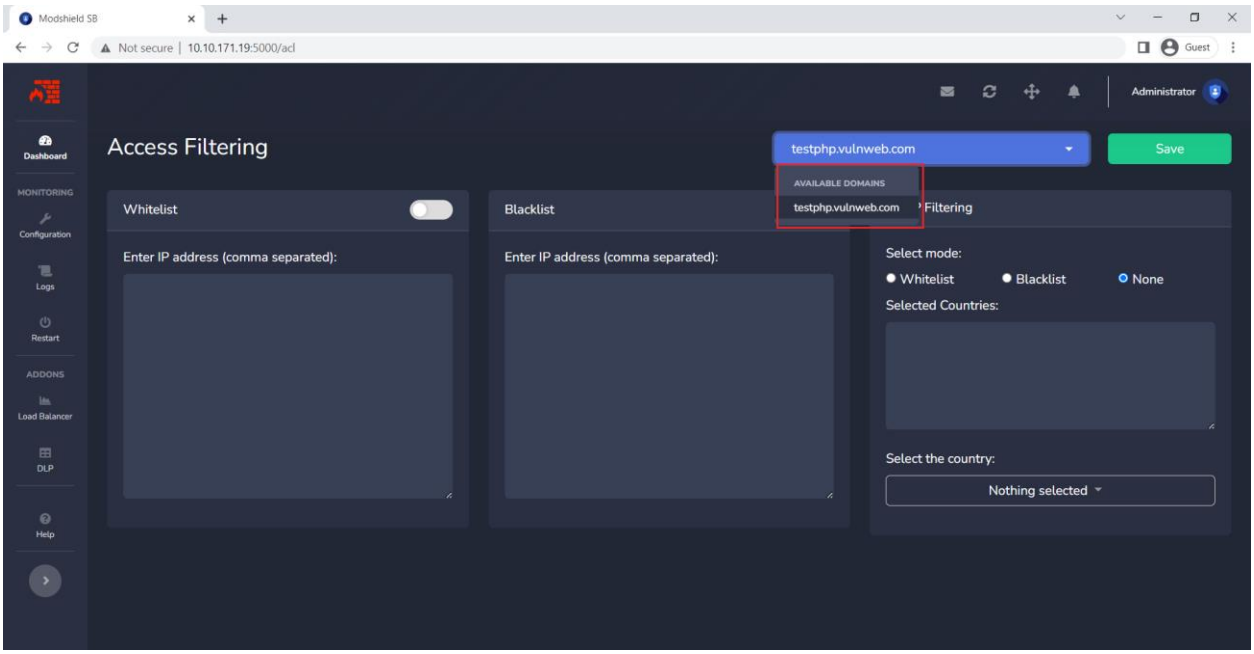
This is done by using a set of whitelists or blacklists.



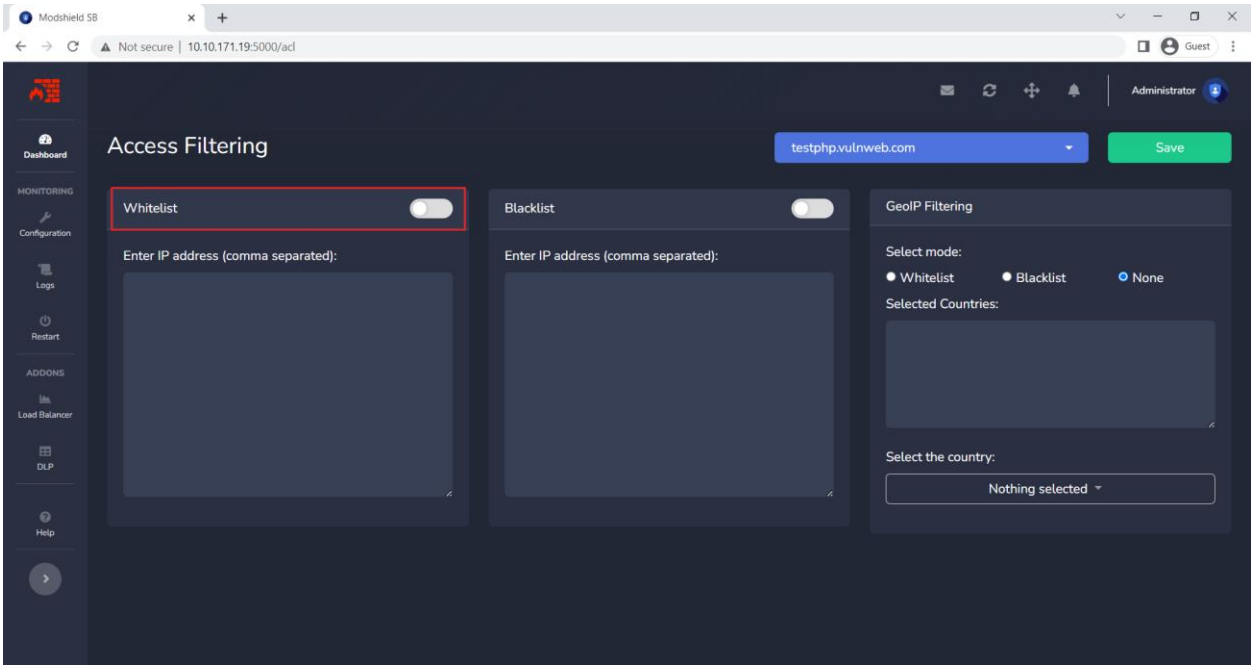
Modshield allows you to restrict IPs, IP ranges and countries. You can specify this for each domain



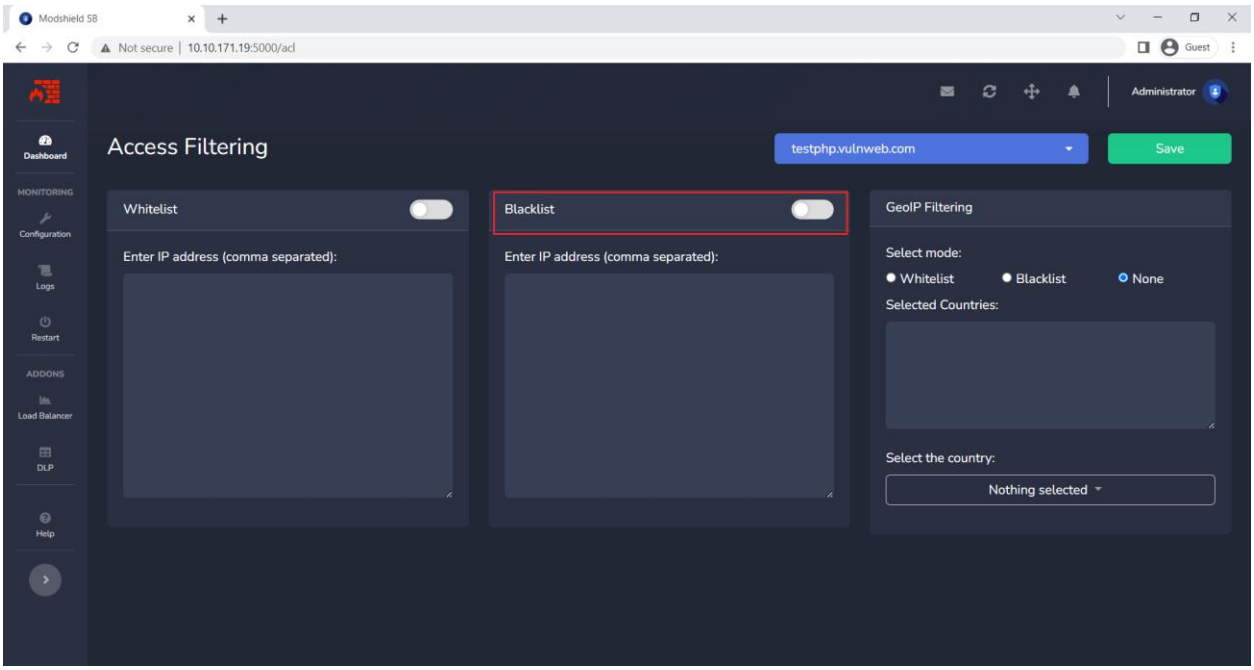
To begin, select the domain for which you would like to restrict access



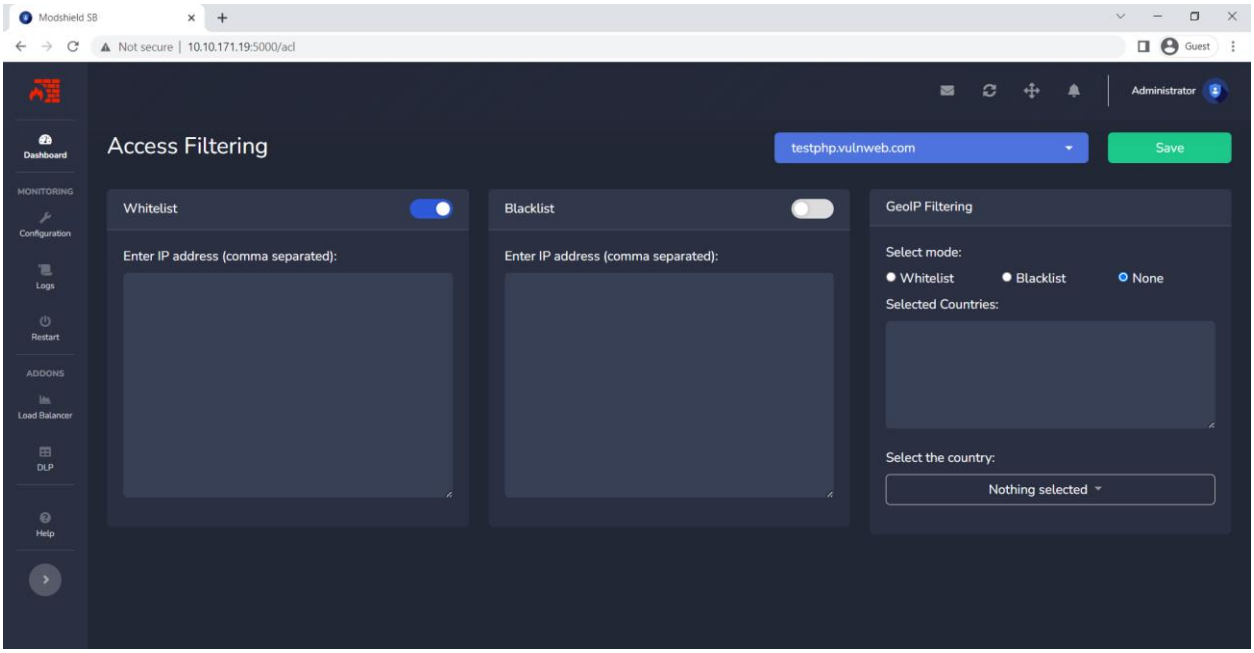
Whitelists allow traffic only from the IPs mentioned in the list. All other IPs are blocked



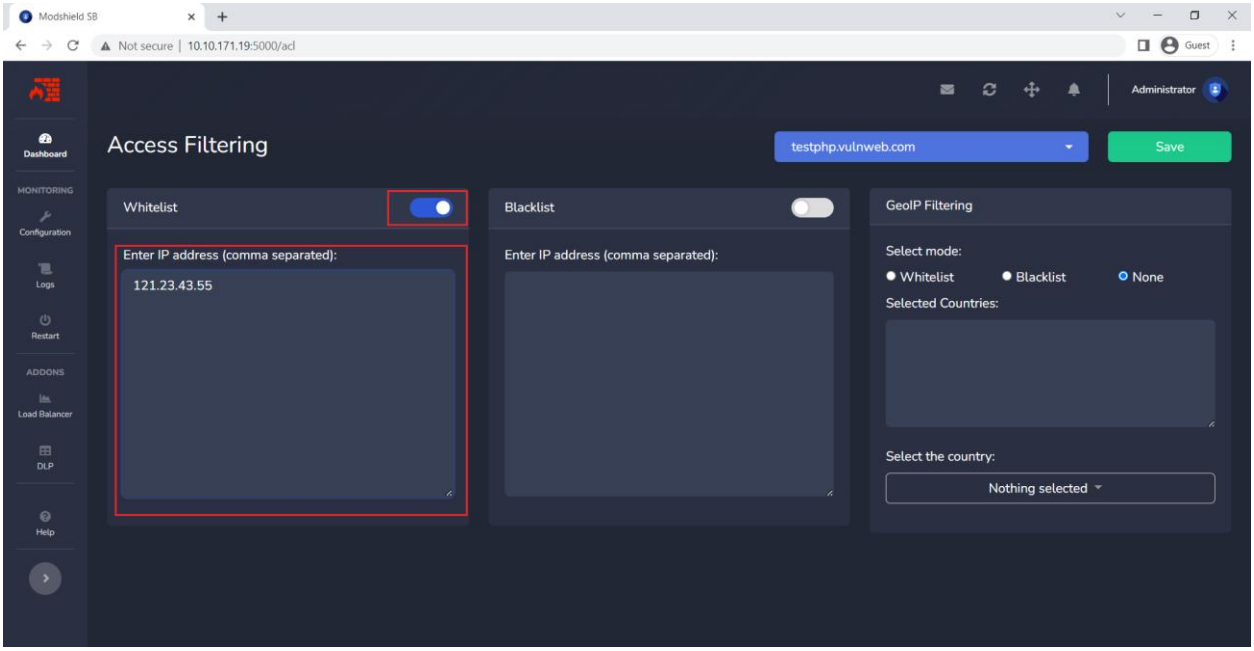
Blacklists on the other hand, allow traffic from all IPs other than the ones in the list



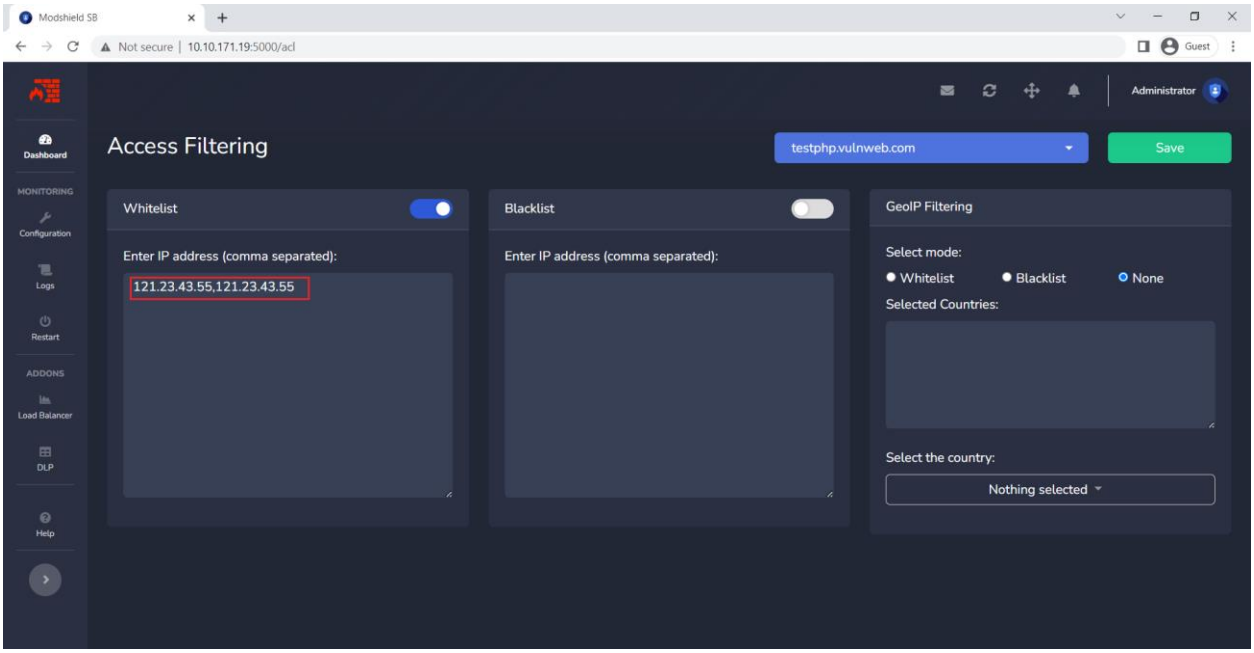
At any given point, you can only have one of these enabled



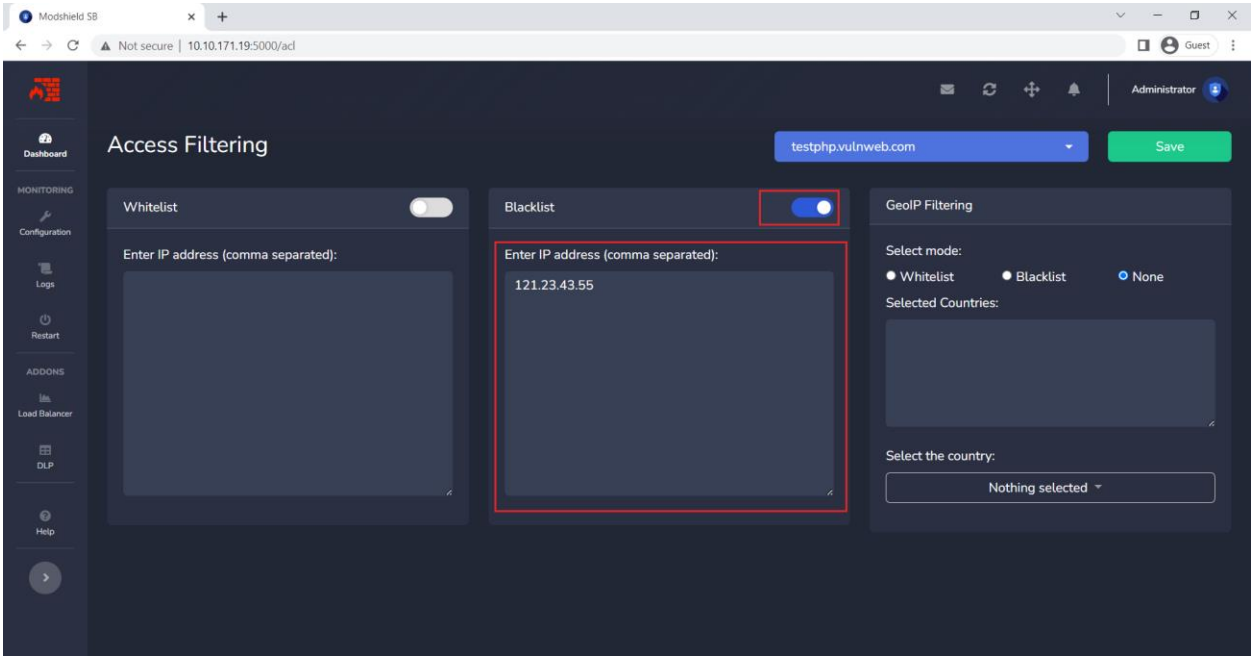
Turn on the Whitelist and enter the IP address that should be whitelisted



Add additional IPs separated by comma

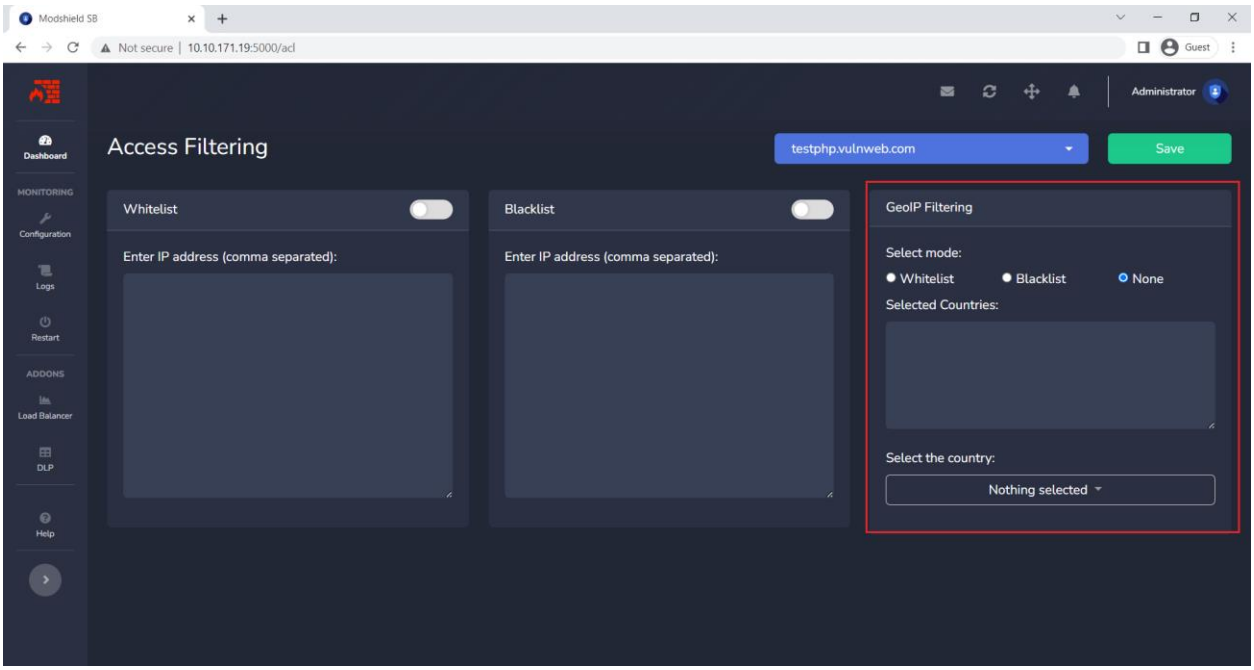


Turning on the Blacklist will automatically disable the whitelist. Add IP addresses to this list in the same way as you did for a whitelist

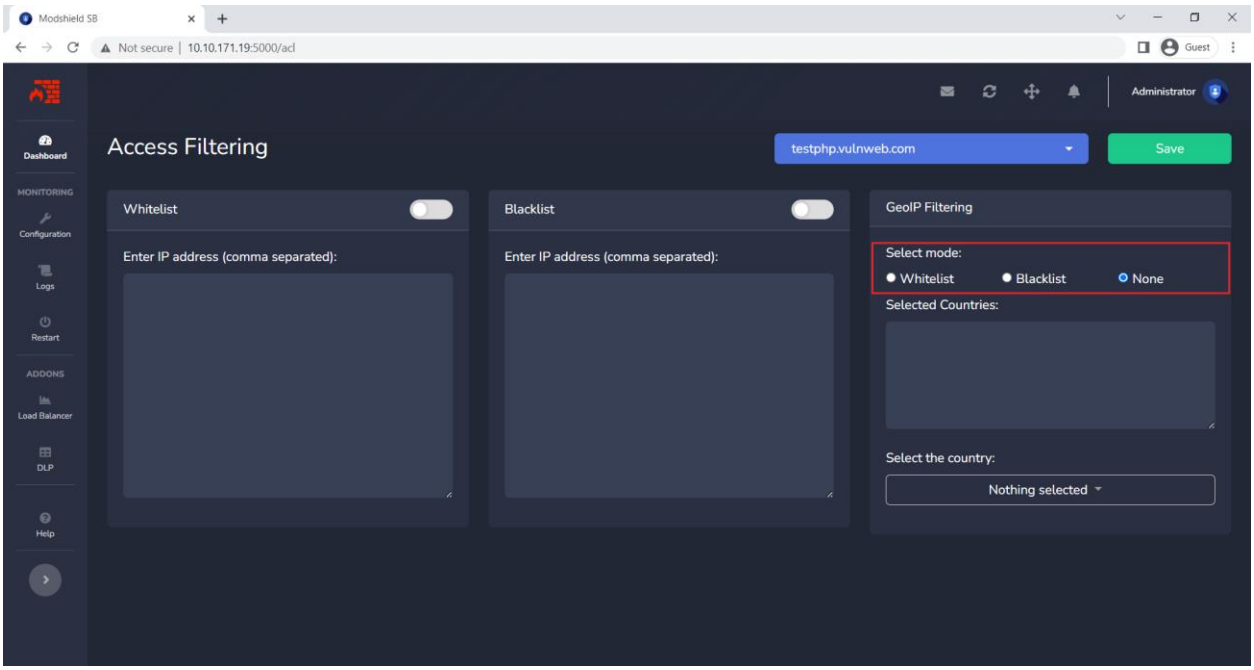


Geo IP Filter

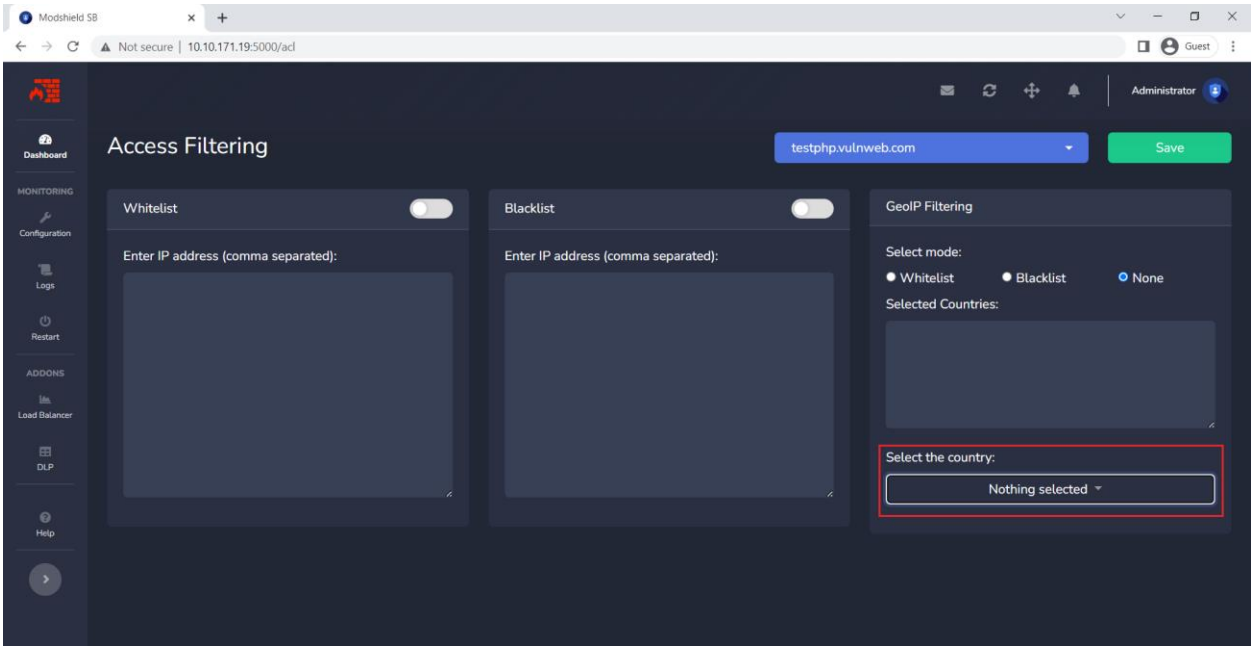
Similarly, you can all restrict IPs from a country or countries using the Geo IP filter.



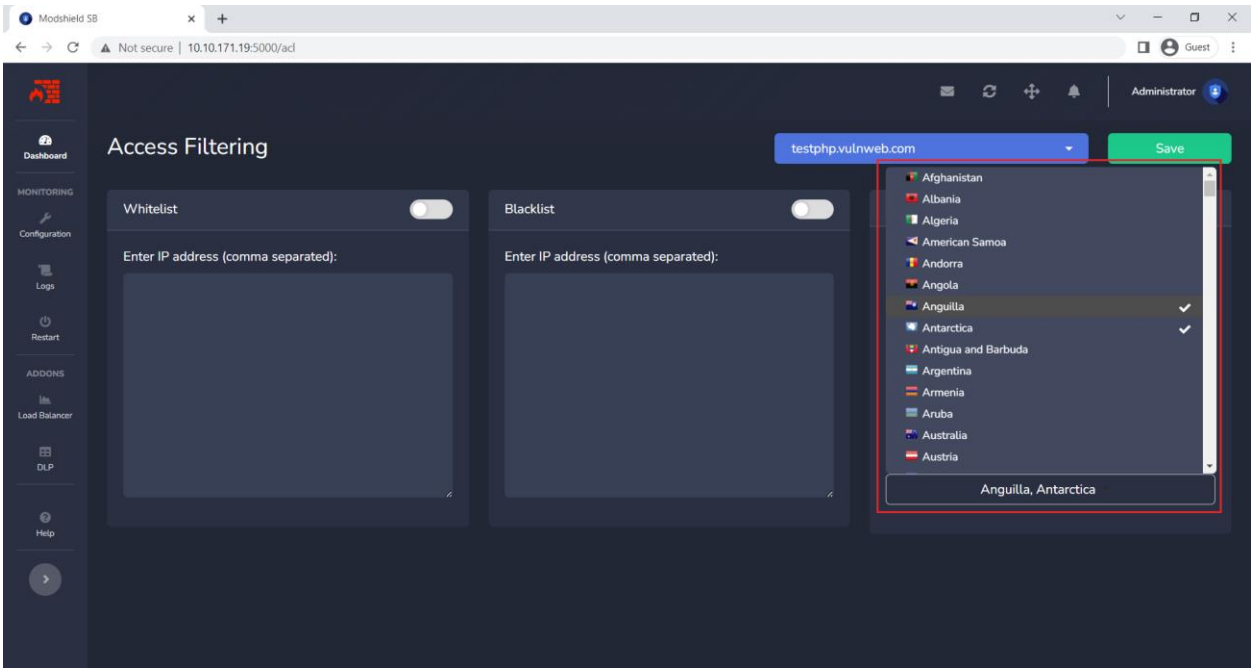
You can choose either to blacklist or whitelist countries



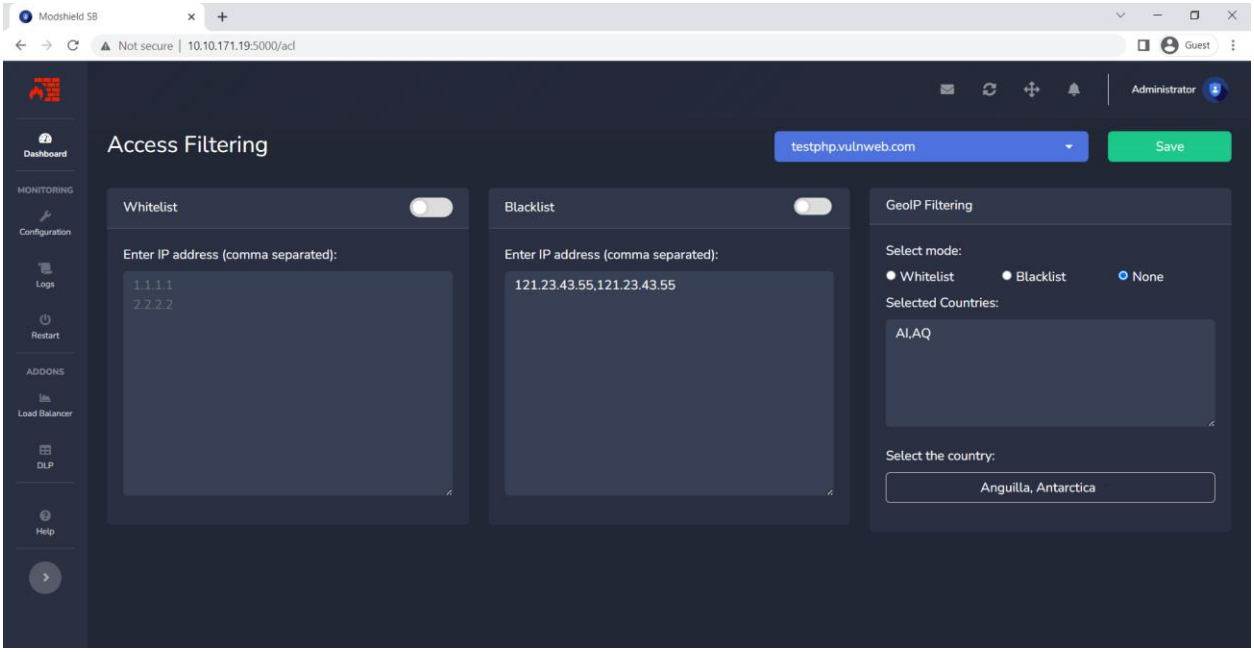
Select the countries that you would like to add to your list



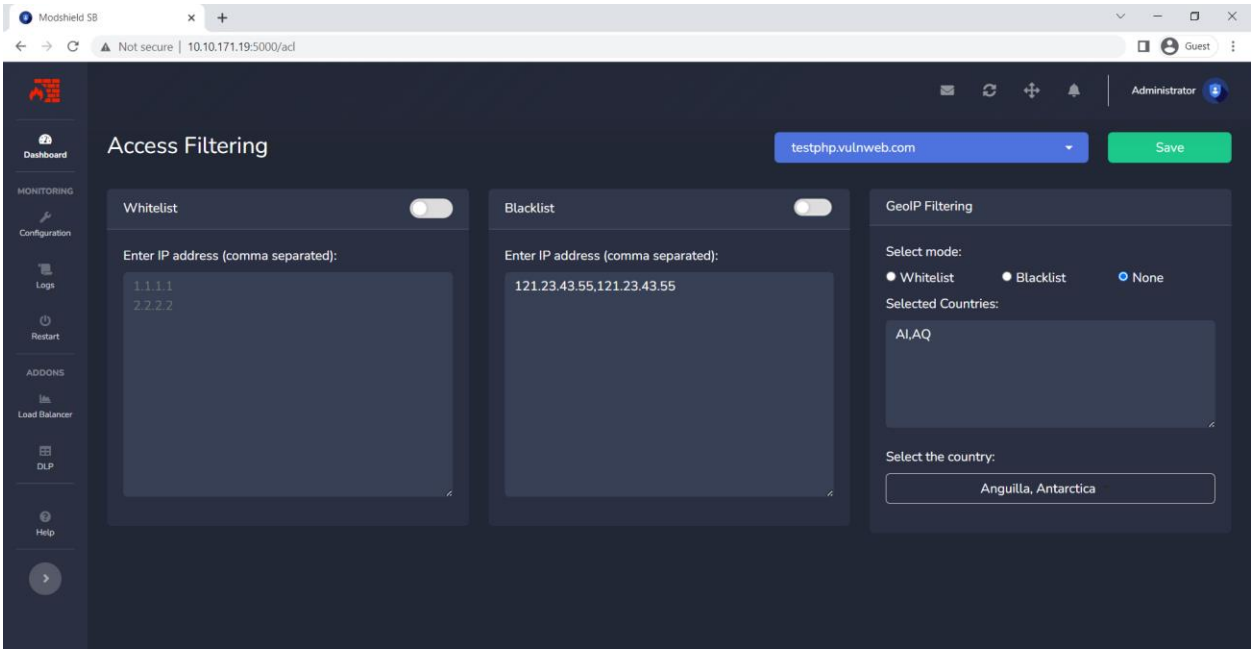
You can choose any number of countries to be added to this list



You can also disable all lists and save the settings to preserve the lists.



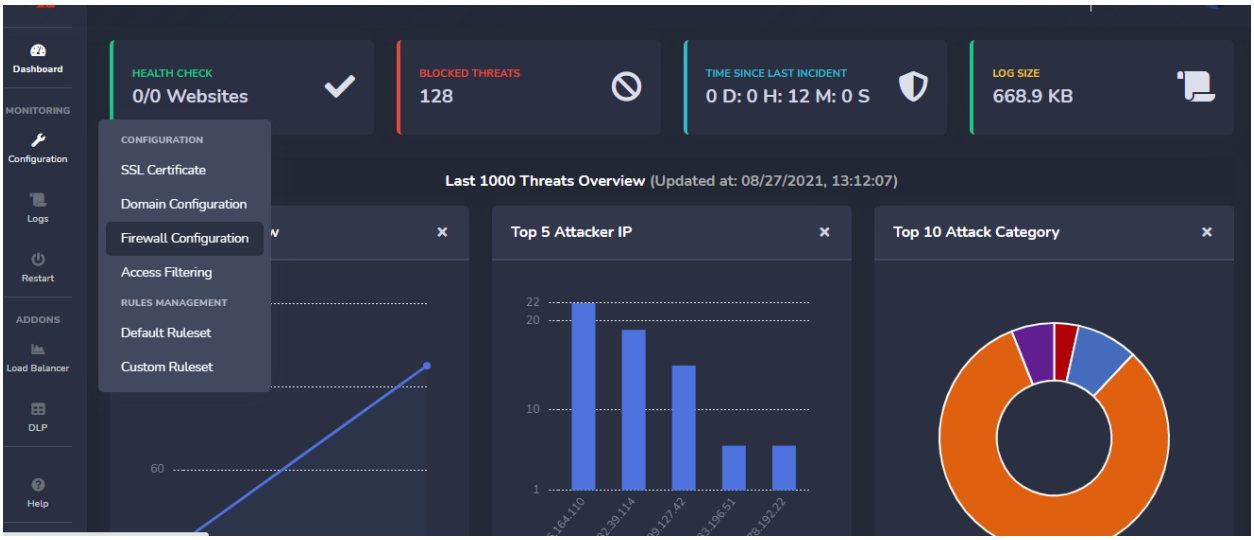
You are not required to remove the entries. This makes it easier to enable the same settings later



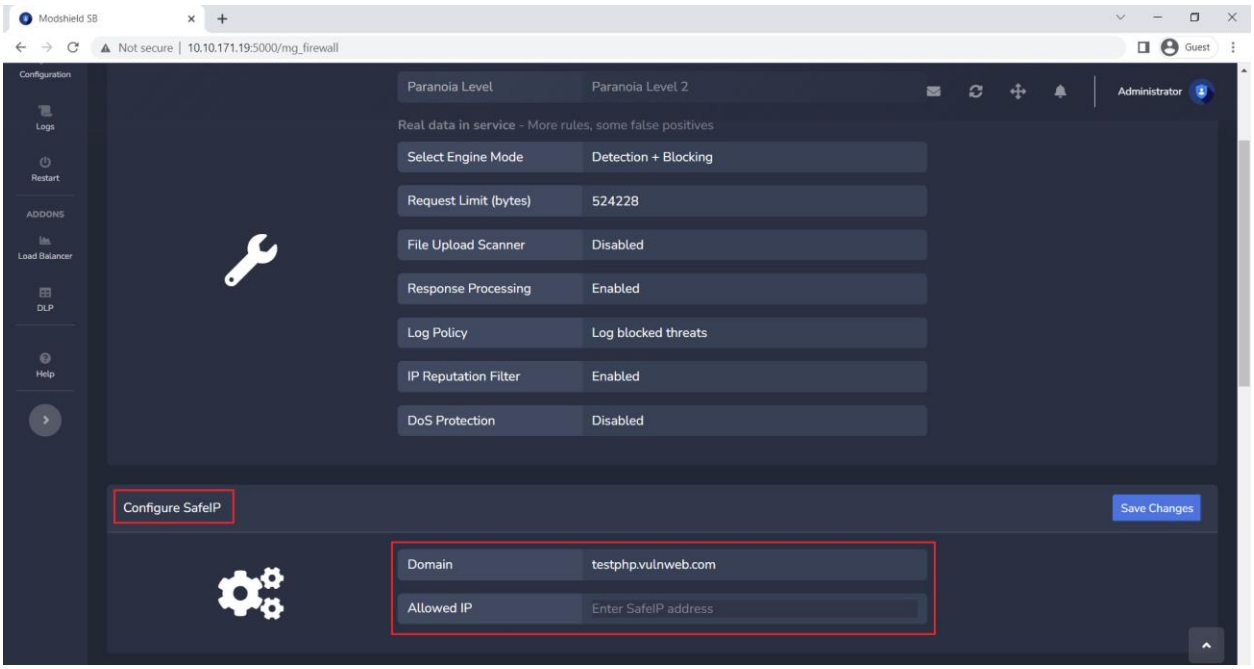
Safe IP

Another setting that provides IP specific access is called a Safe list (Safe IP)

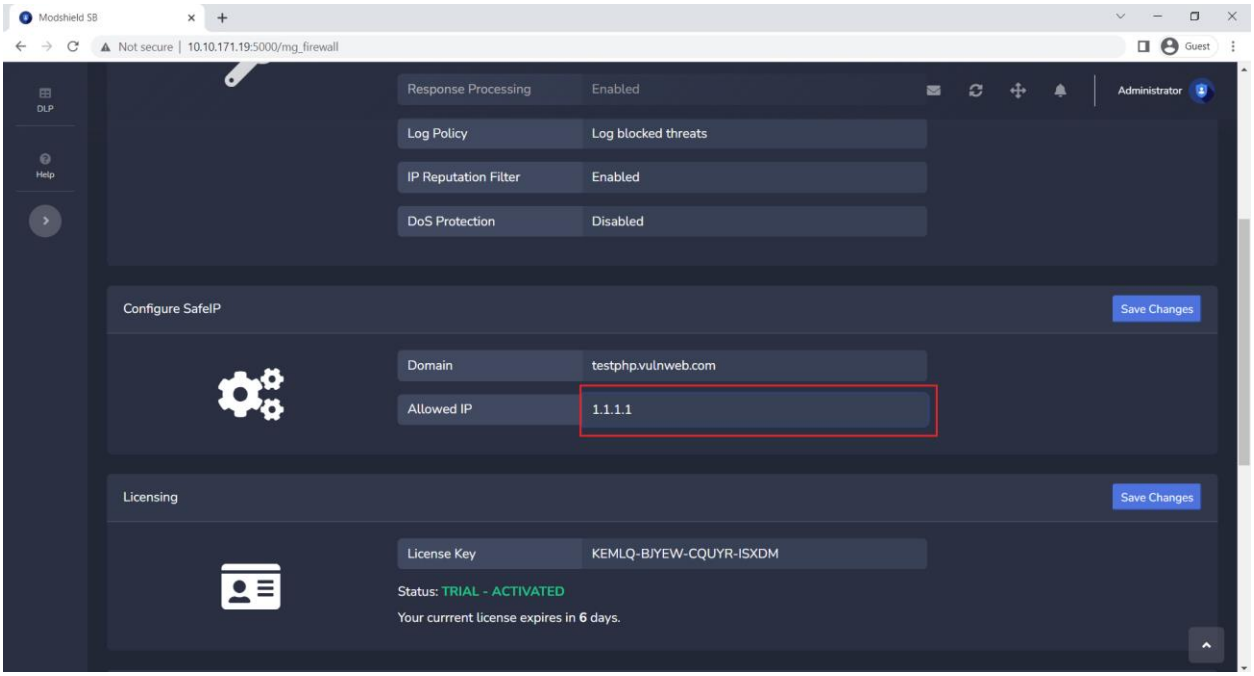
Safe list is found in the firewall configuration menu item



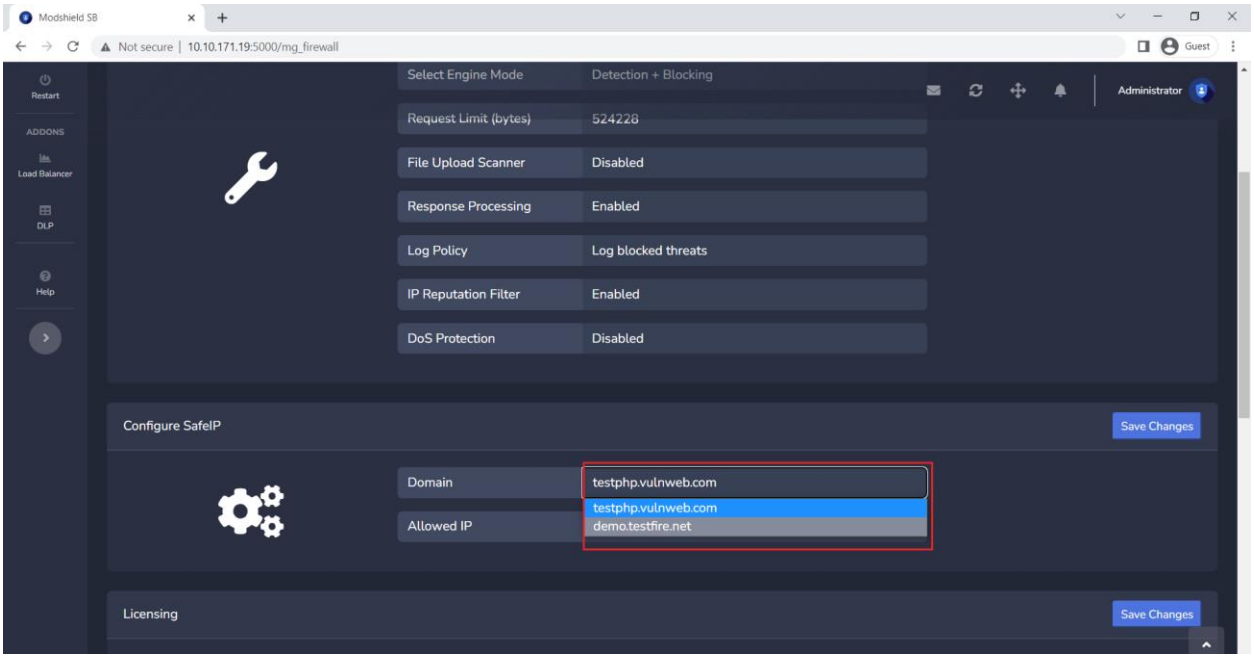
Scroll down to the Safe IP section



You can specify Safe IPs for each of the domain that you manage

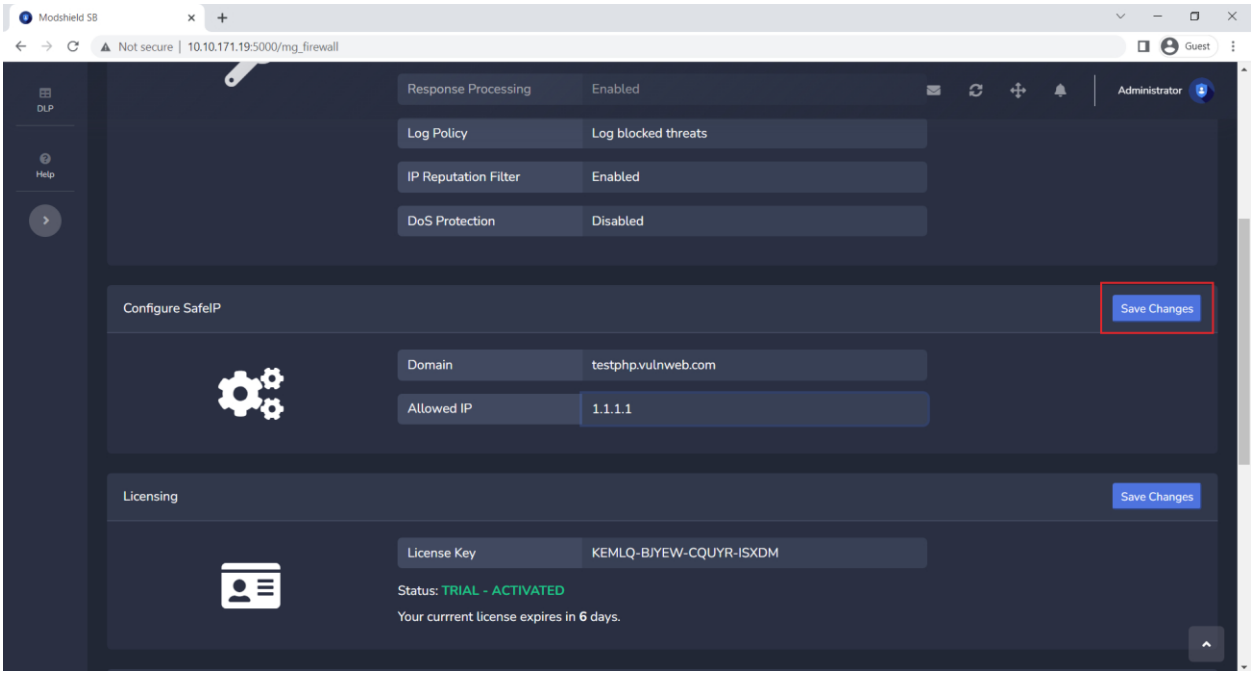


Modshield will turn off the rules processing for all traffic from this IP address alone



It is important to ensure that the safe IP is not blocked by any whitelist or blacklist settings

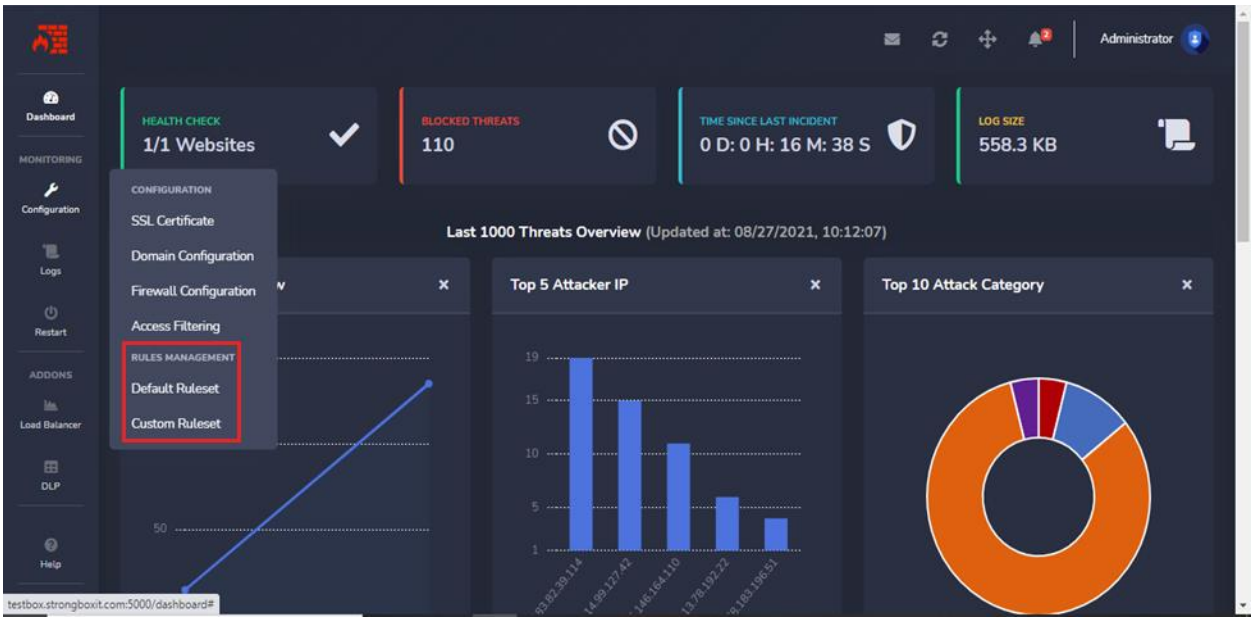
As always, please save changes for the settings to take effect



Rules Management

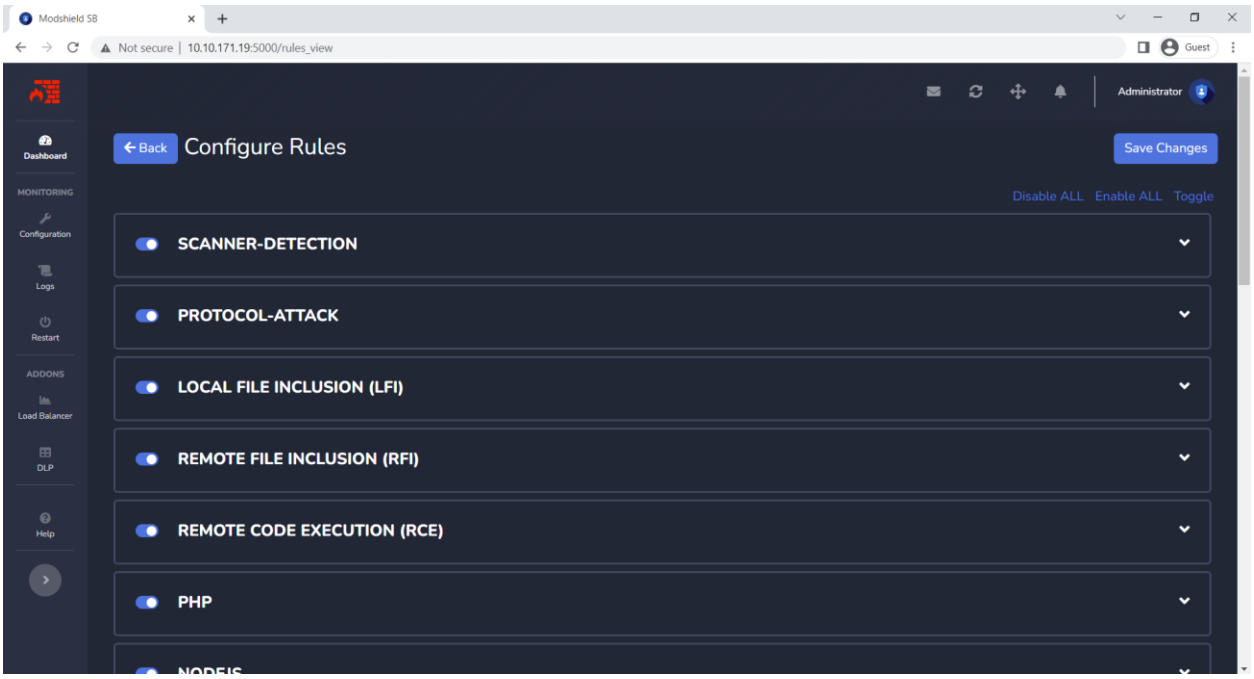
Video Link: https://youtu.be/qp1VvIu4oOs.

Modshield has a built-in set of rules that enable effective protection against all common attacks

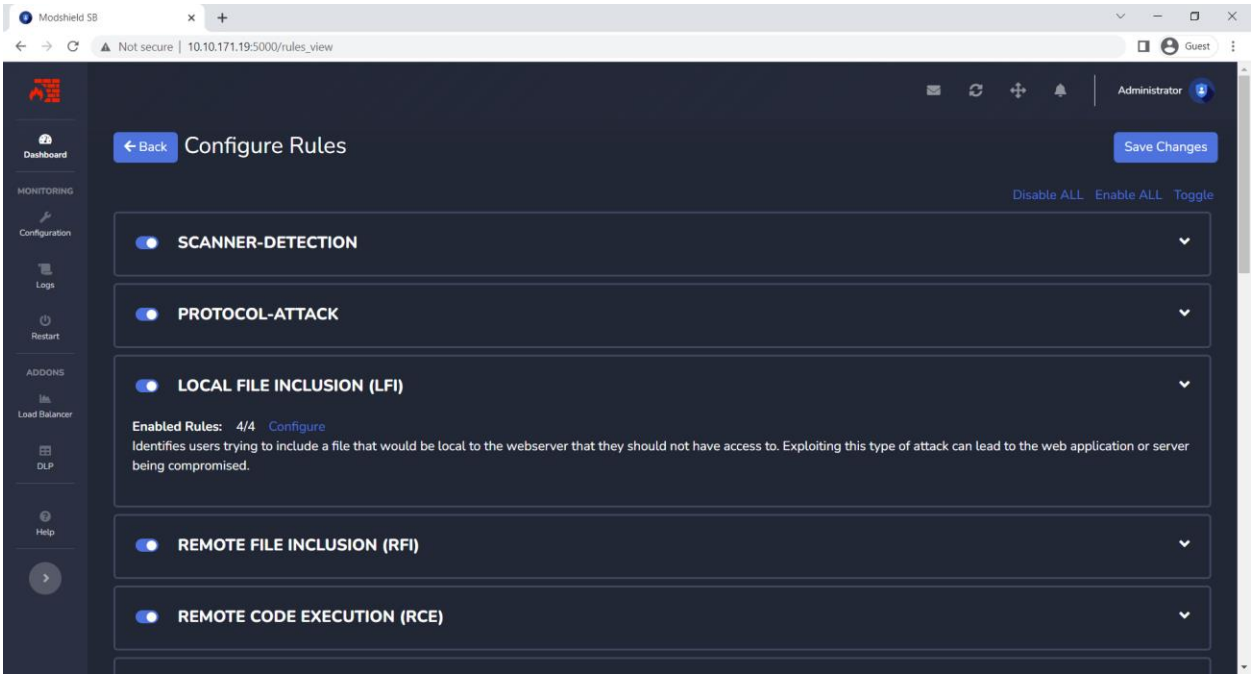


Default Rulesets and Rules

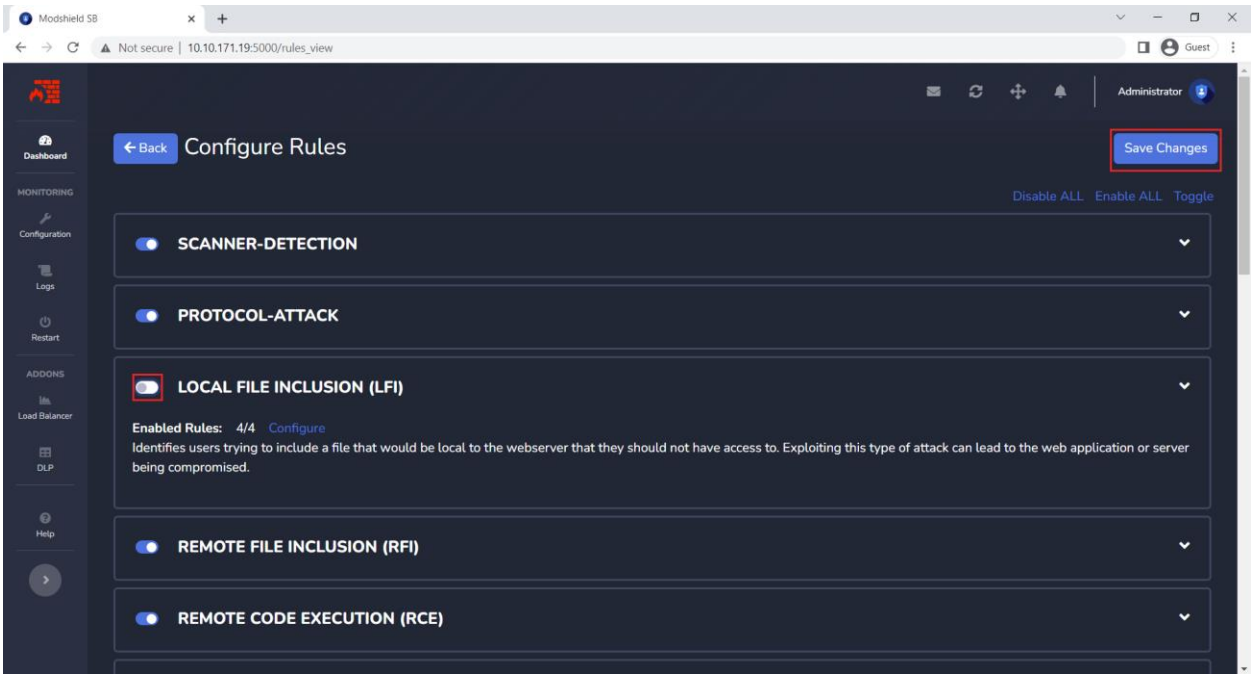
To view and configure the default set of rules that are provided, open the default ruleset from the configuration menu



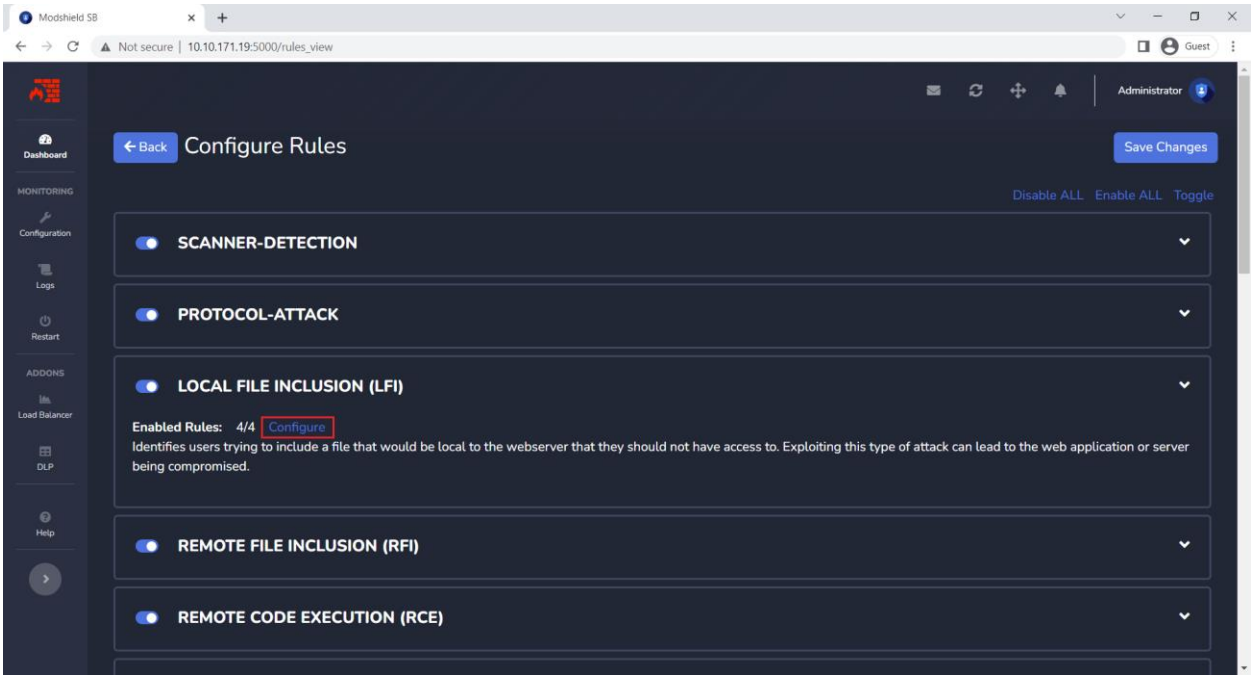
Expand the ruleset by clicking on it. You can see the number of rules enabled in that set\\



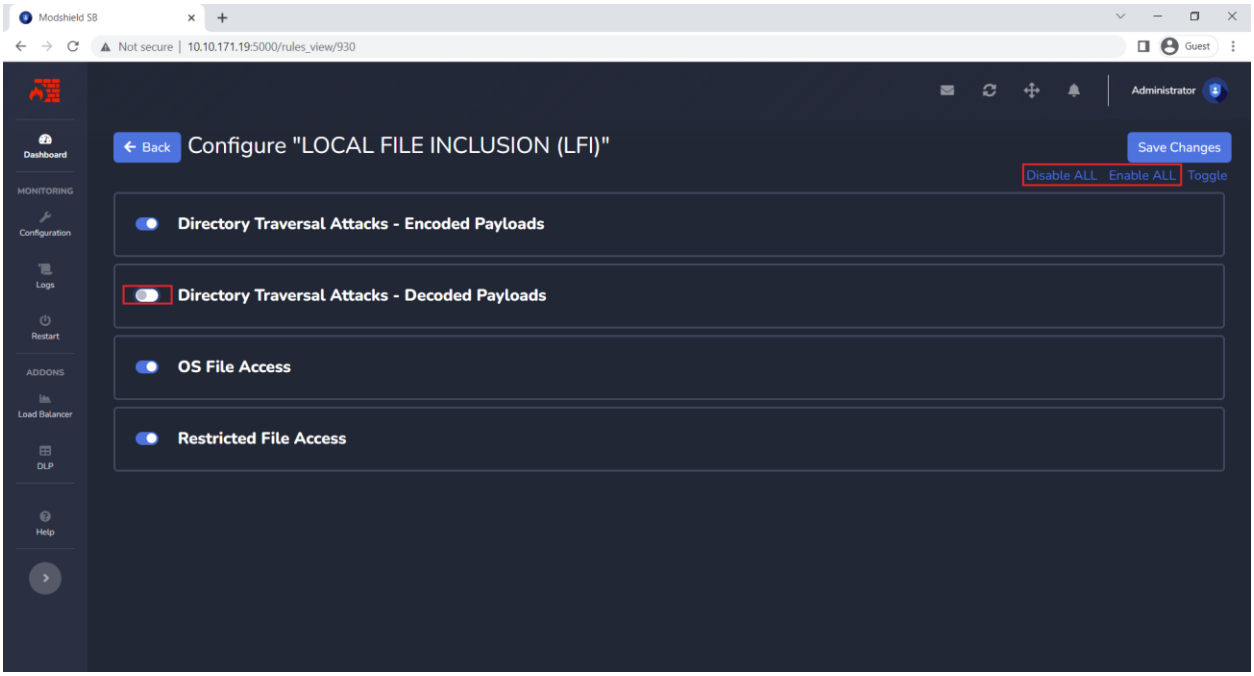
You can choose to disable the rulesets as a whole



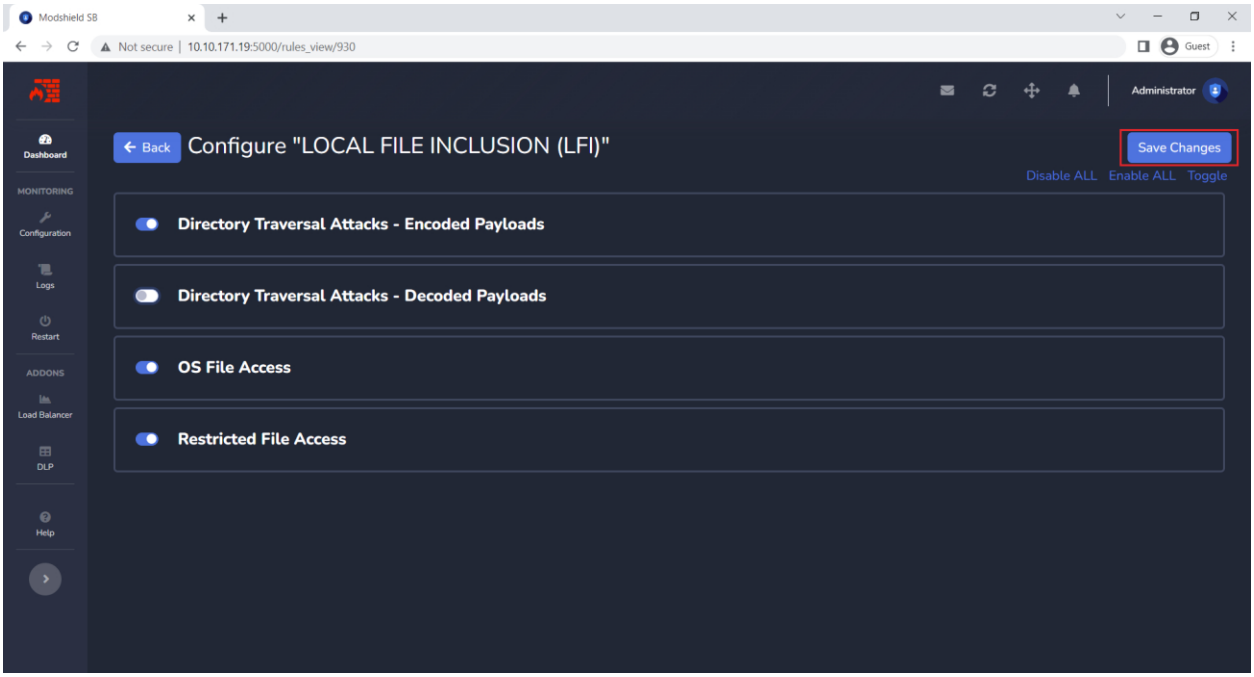
or you can click on configure which then lists all the rules in that ruleset



You can choose to enable or disable individual rules as well as all the rules as whole using Disable ALL or Enable ALL

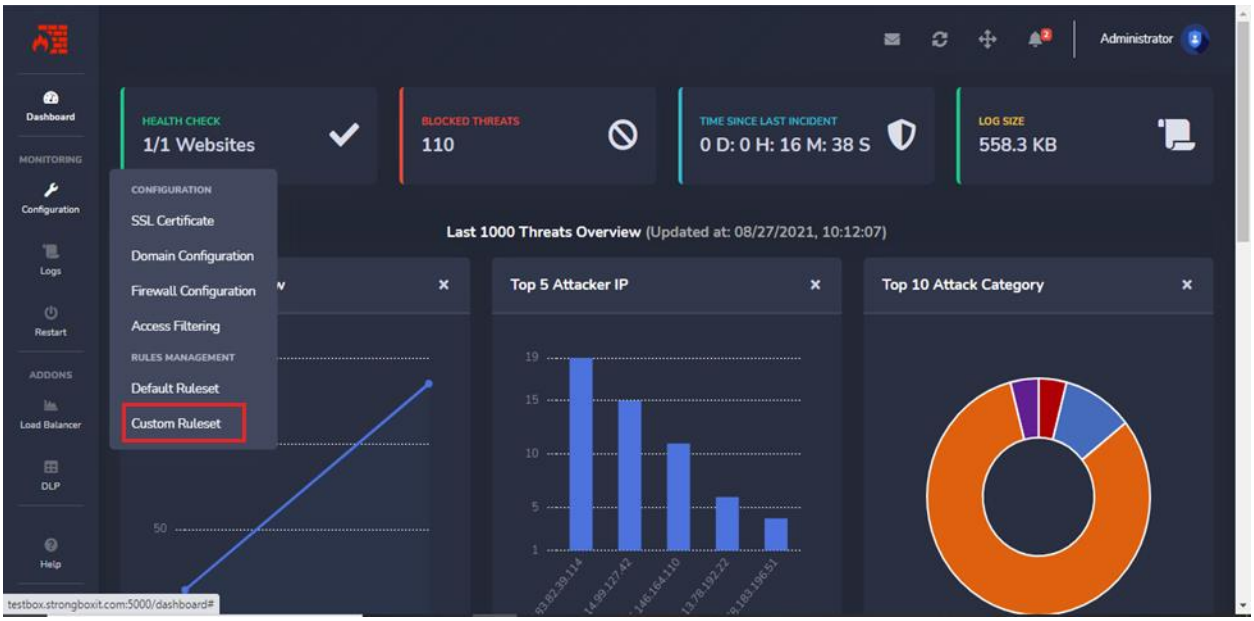


Once done, click on Save Changes to update the rule configurations

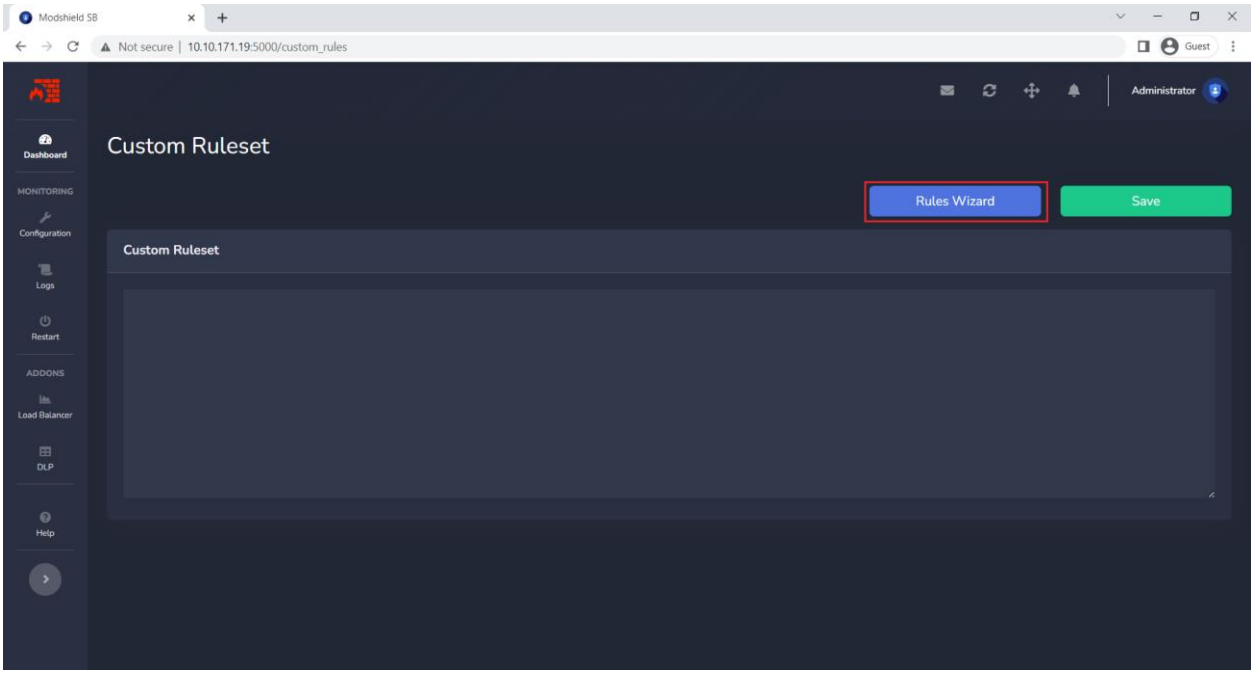


Custom Rules

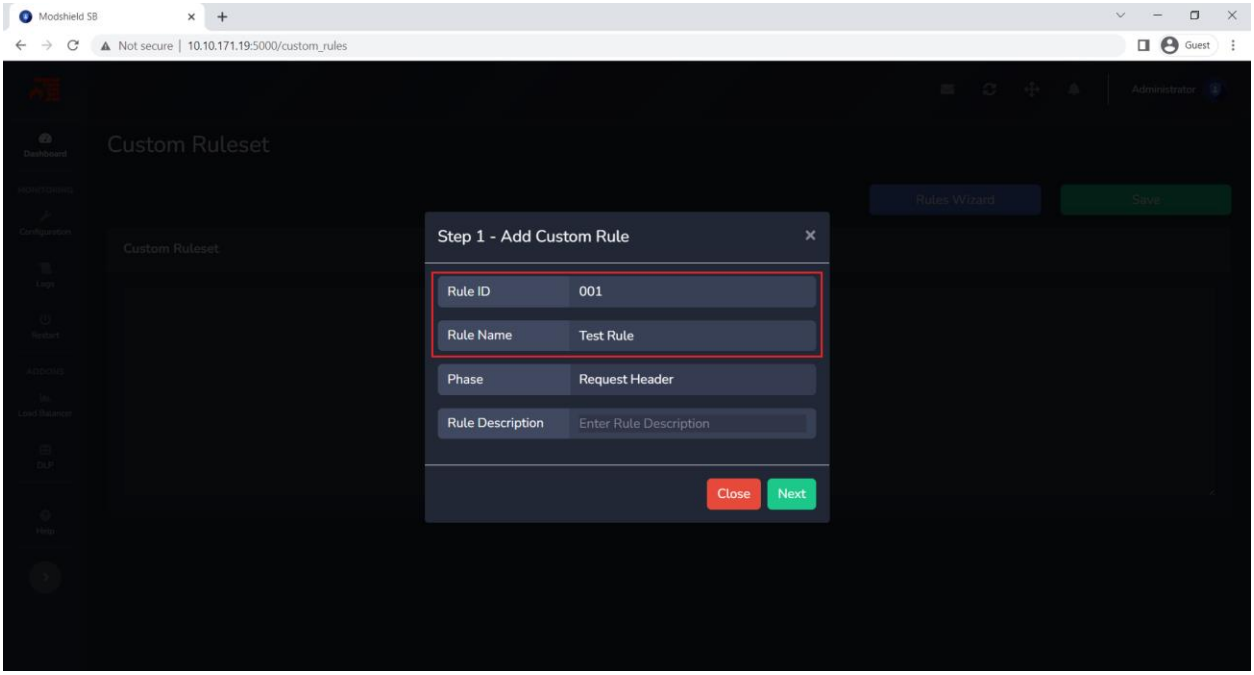
You can add custom rules using the custom ruleset menu in the configuration



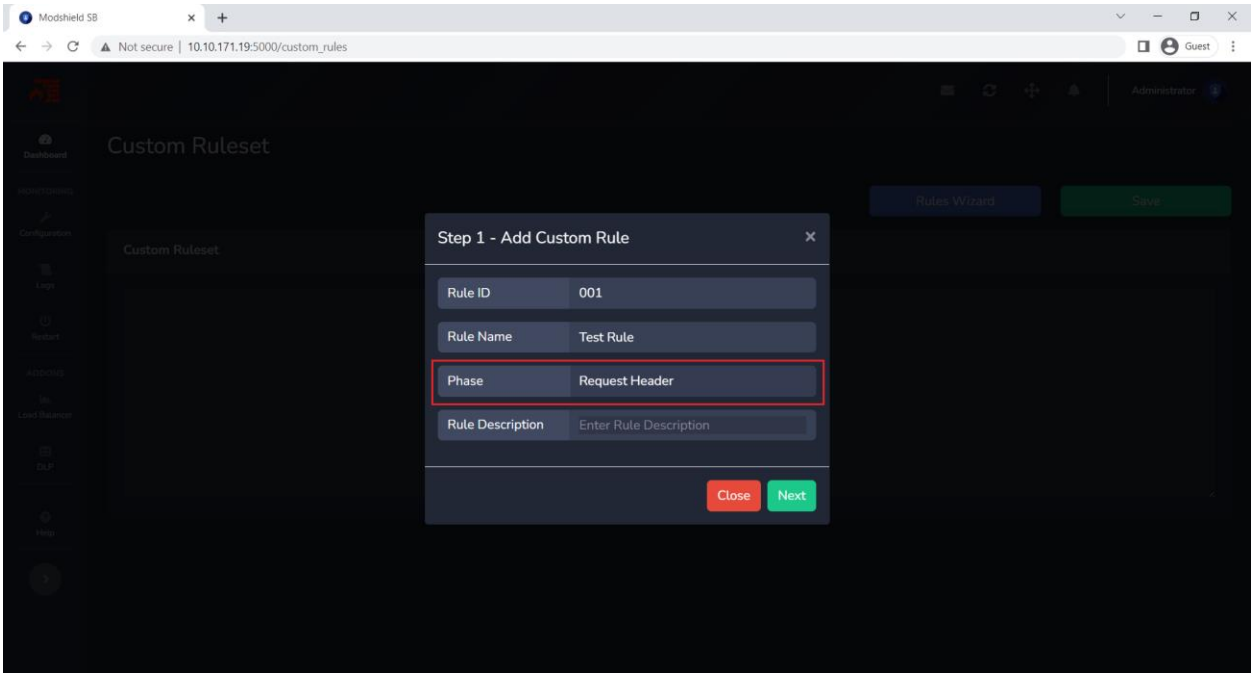
The rules wizard makes it easy for you to add a simple custom rule



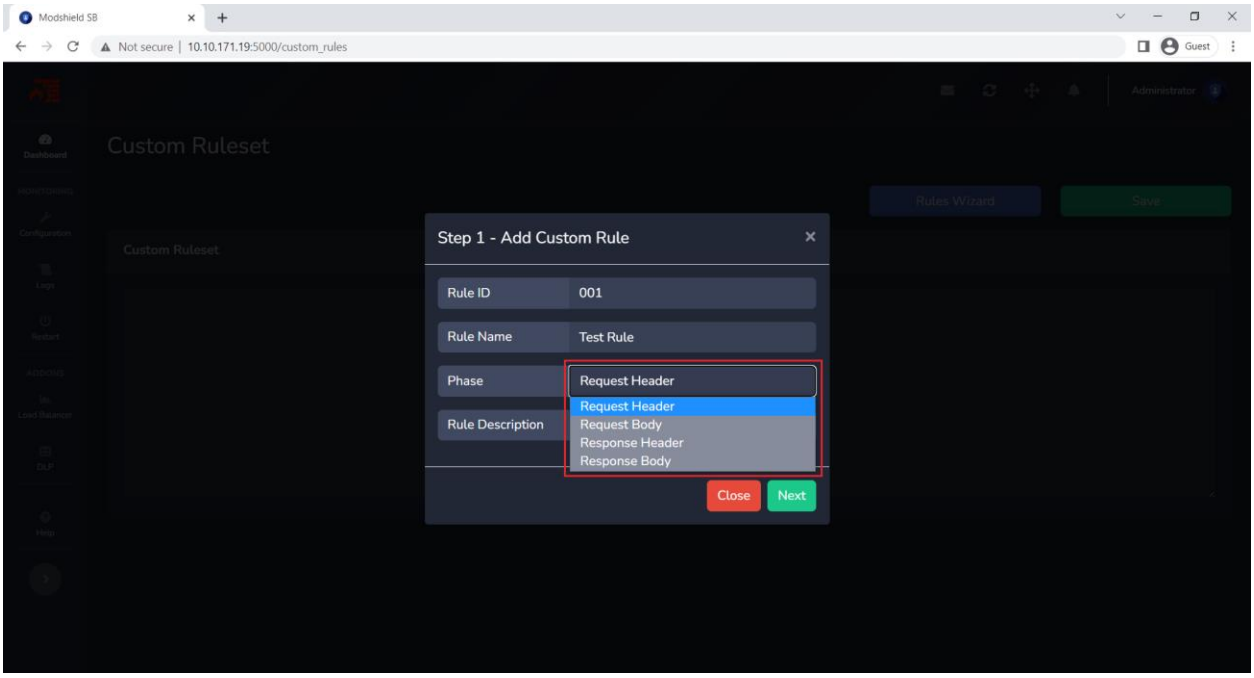
Enter a unique rule ID, a name and choose the phase in which the rule should be applied



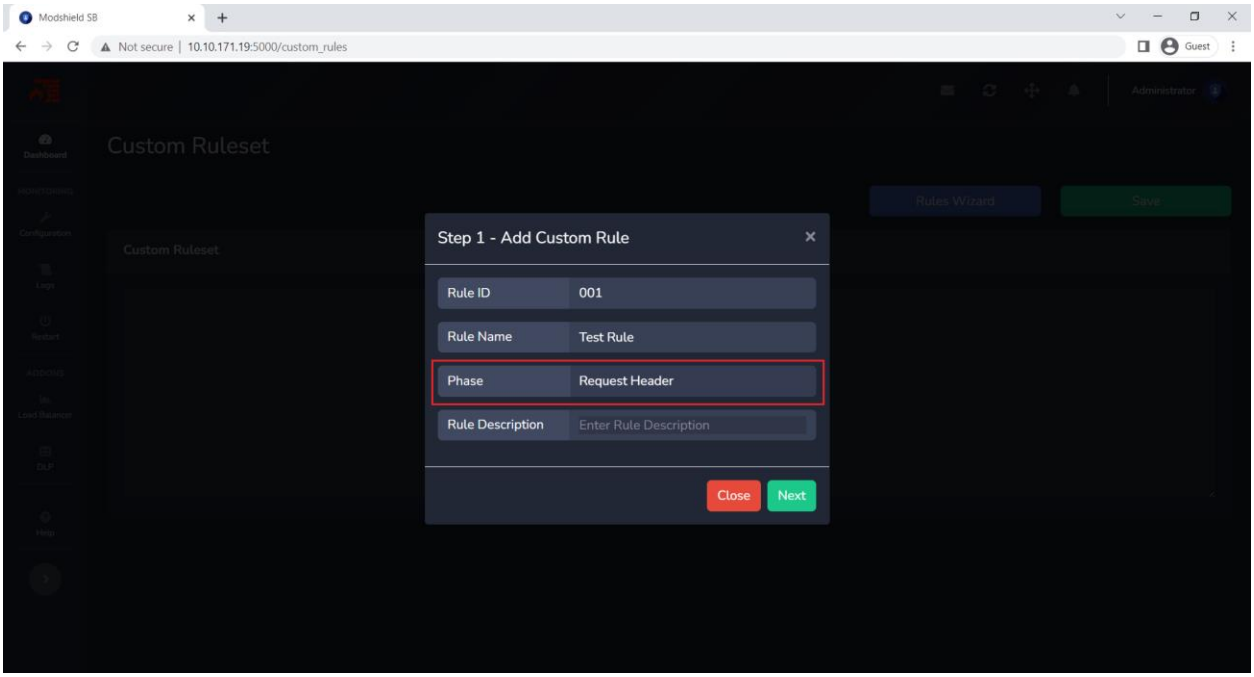
Modshield applies the rules based on the phase in which it is defined



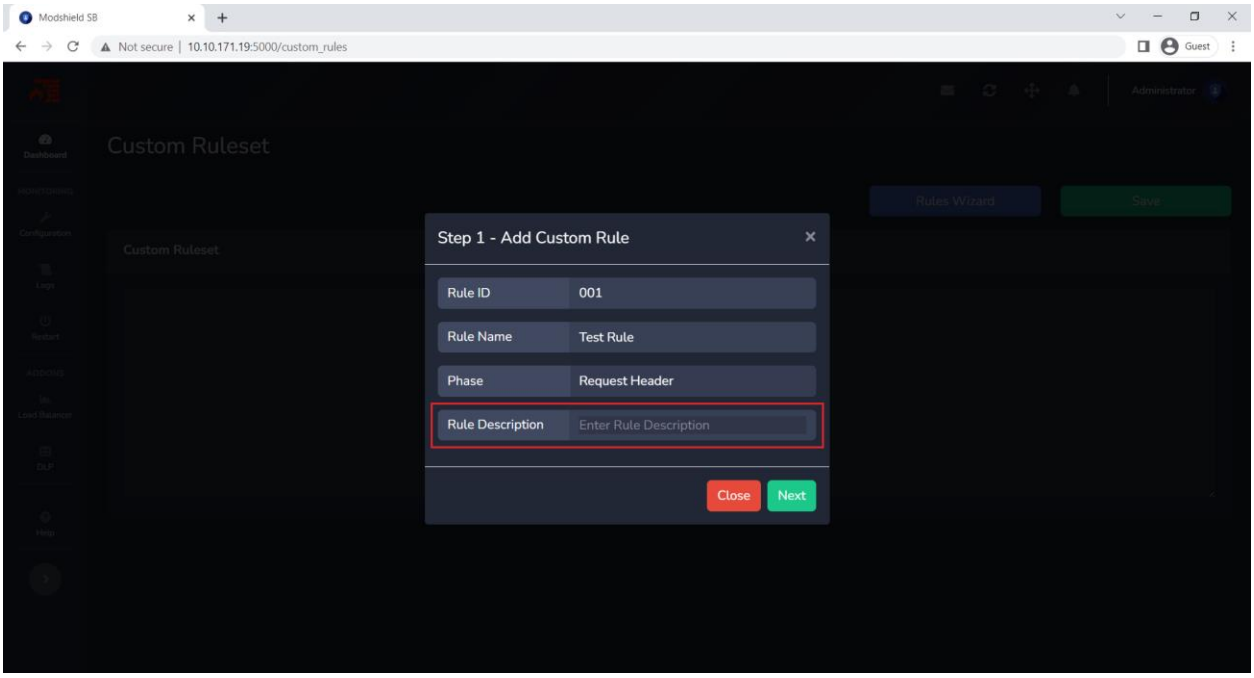
Request header, Body, and Response header, Body are the phases in Modshield



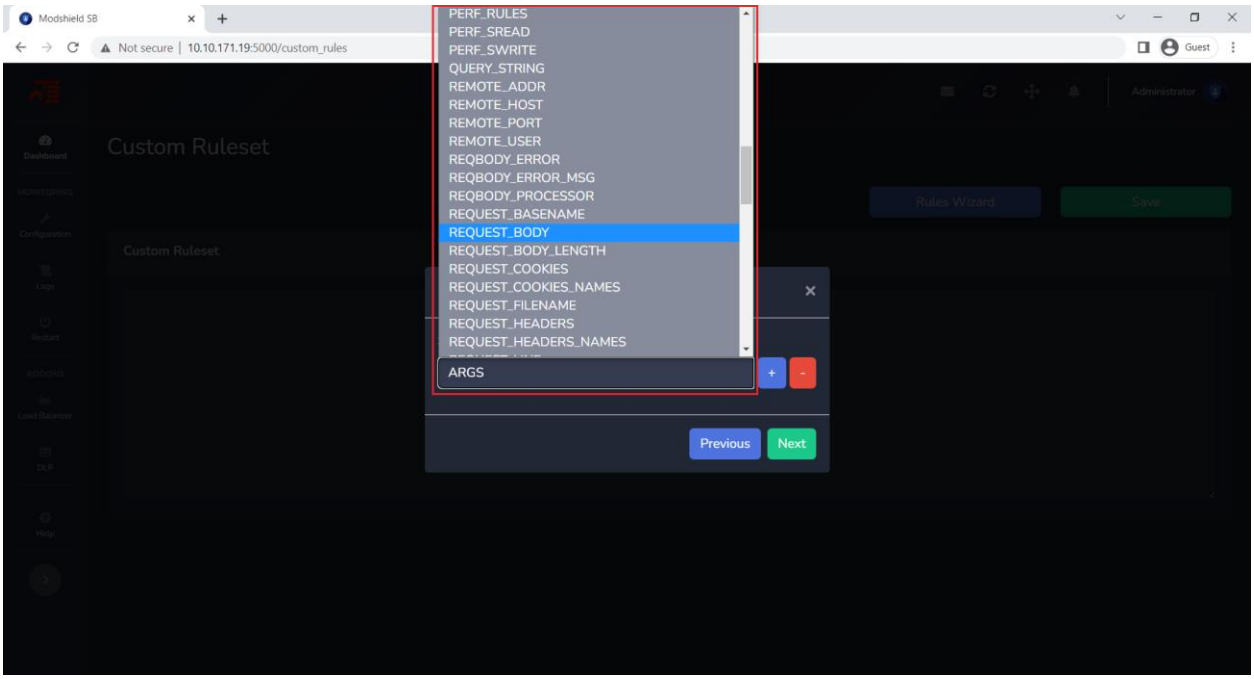
Choose the phase in which this rule should be applied



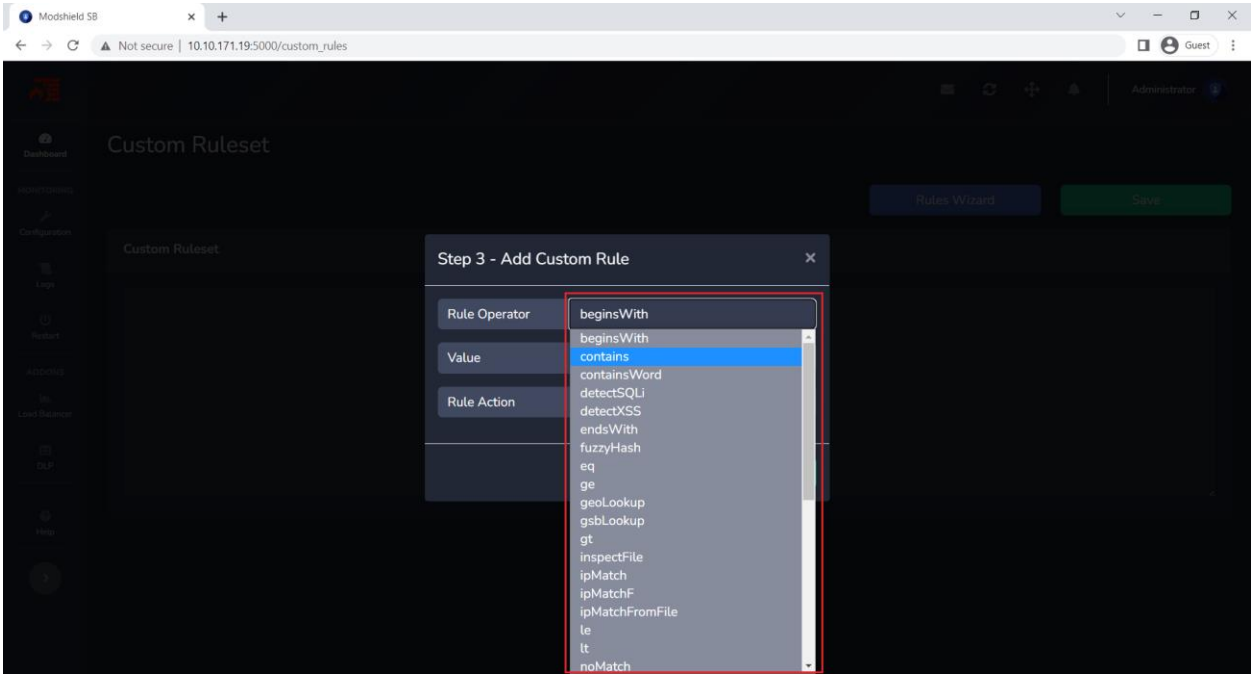
Enter the description. This will be stored as a Message in the log file. Click next



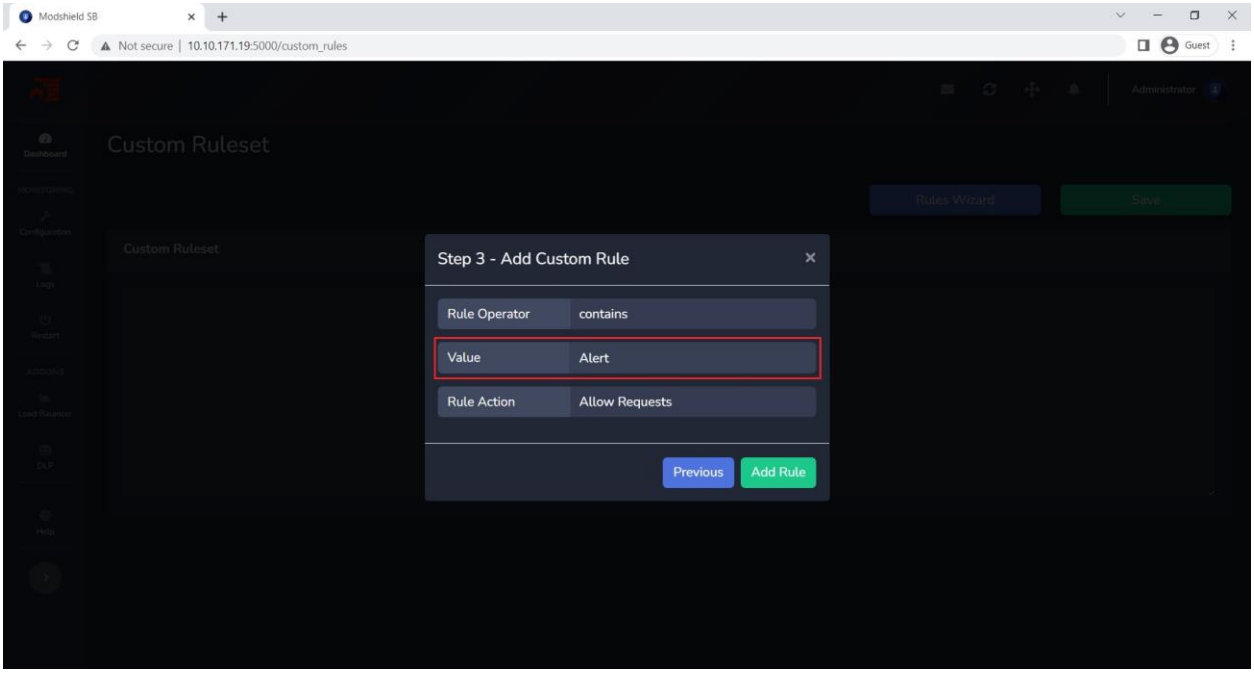
Choose the parameter that the rule is applied on



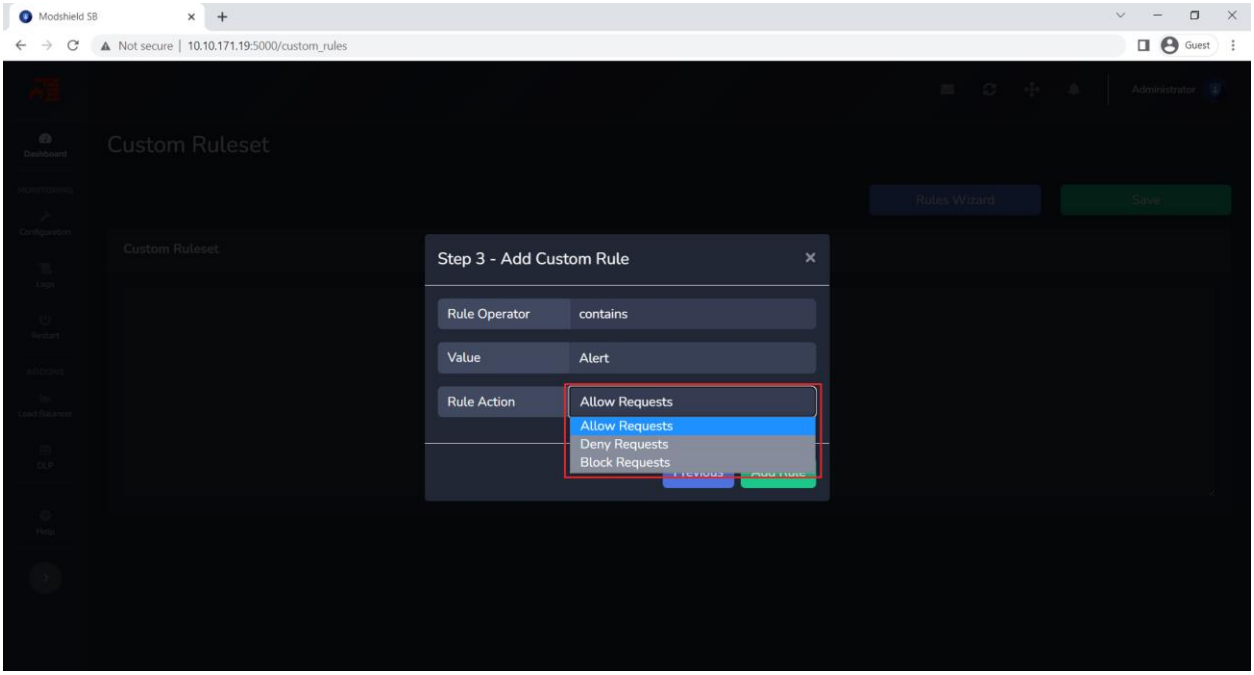
In step 3, select the operation that has to be performed on this parameter



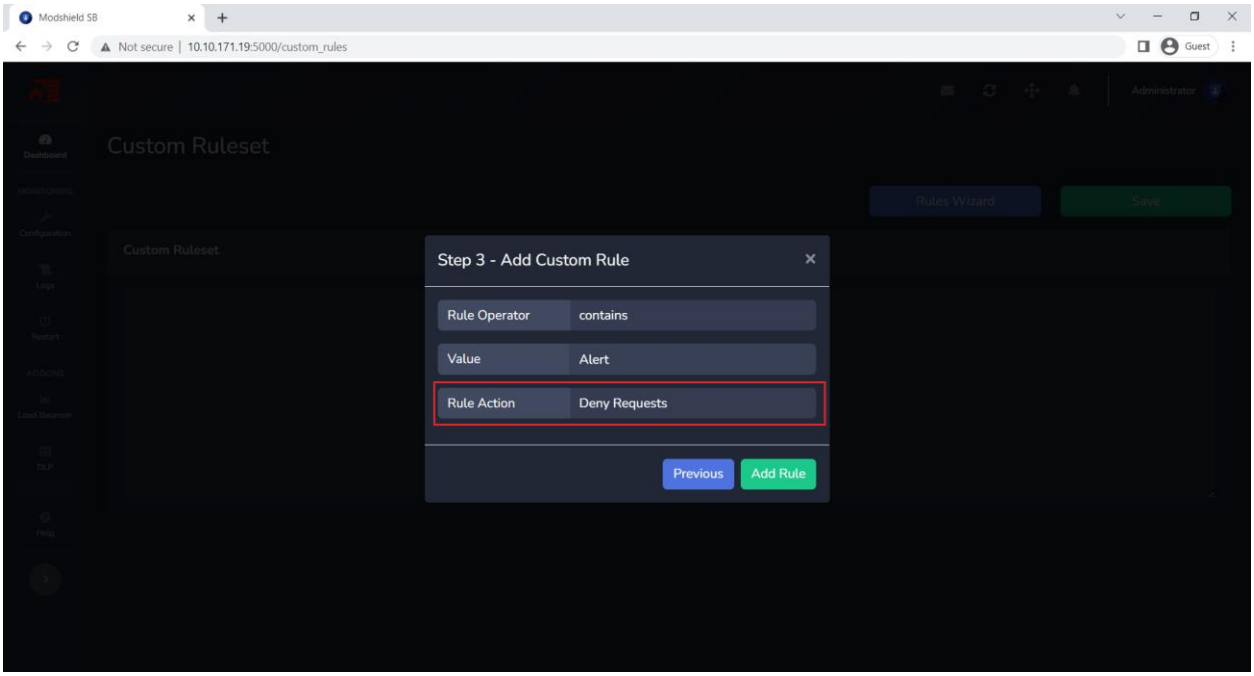
Enter the value against which this parameter has to be compared



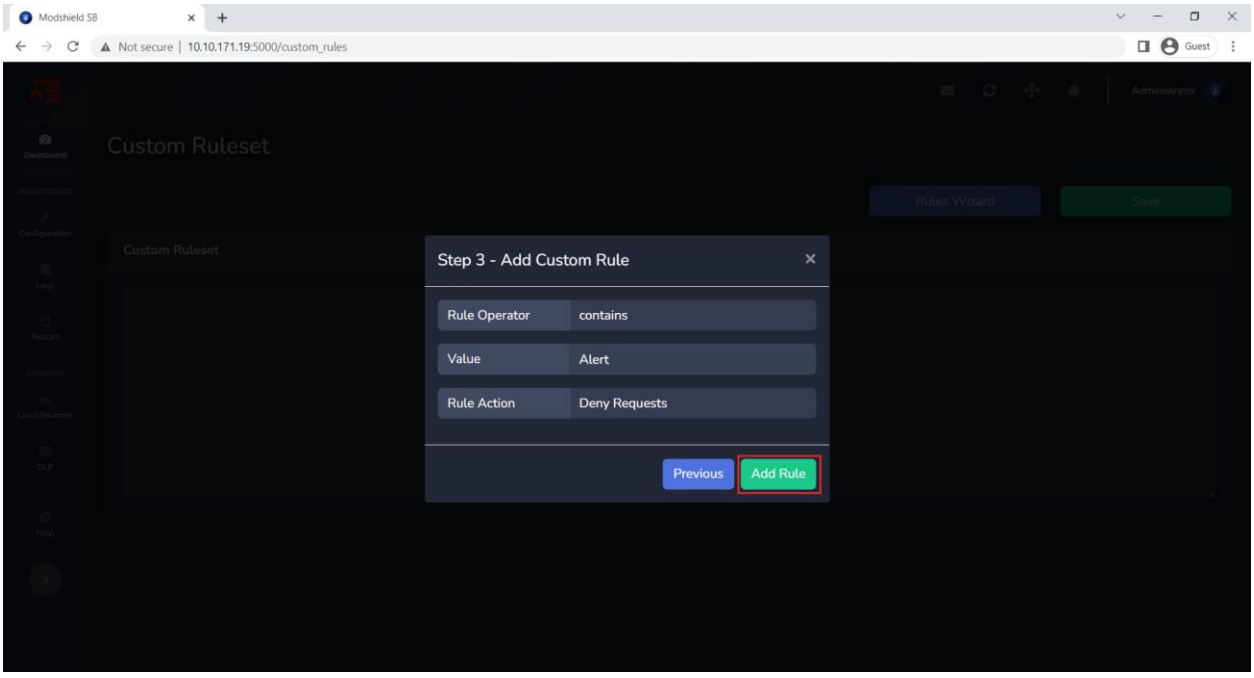
and define the action when the rule matches.



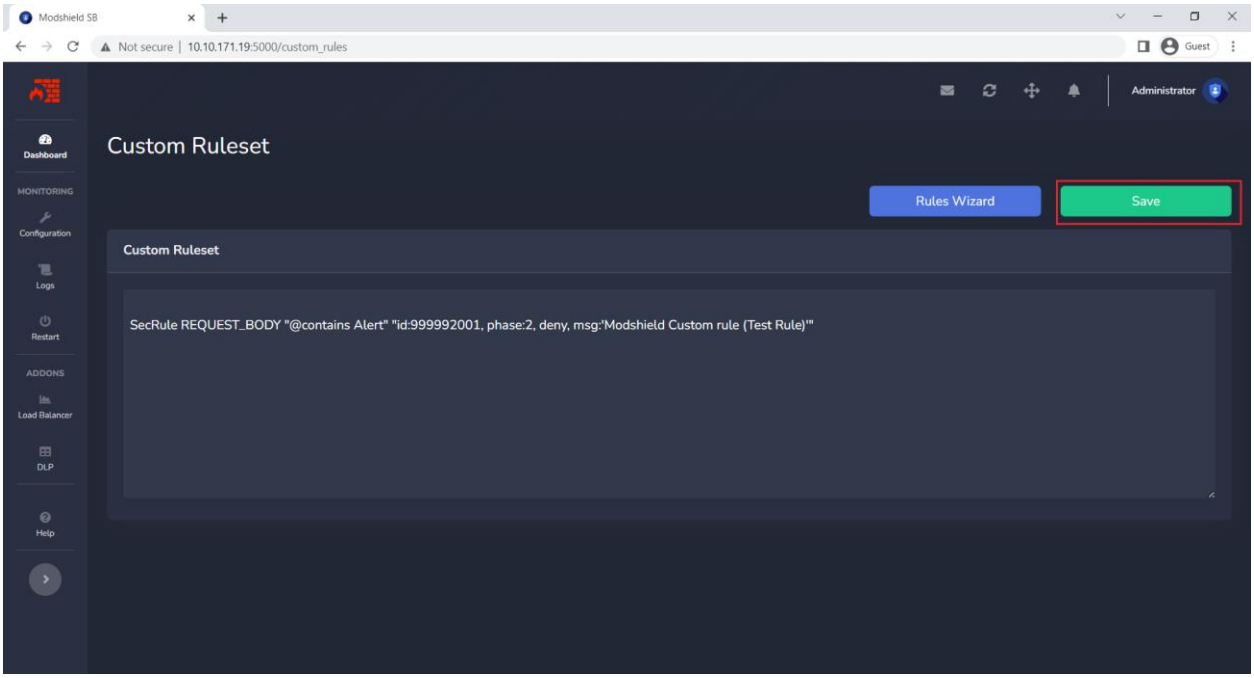
I choose to deny all requests that match the criteria defined



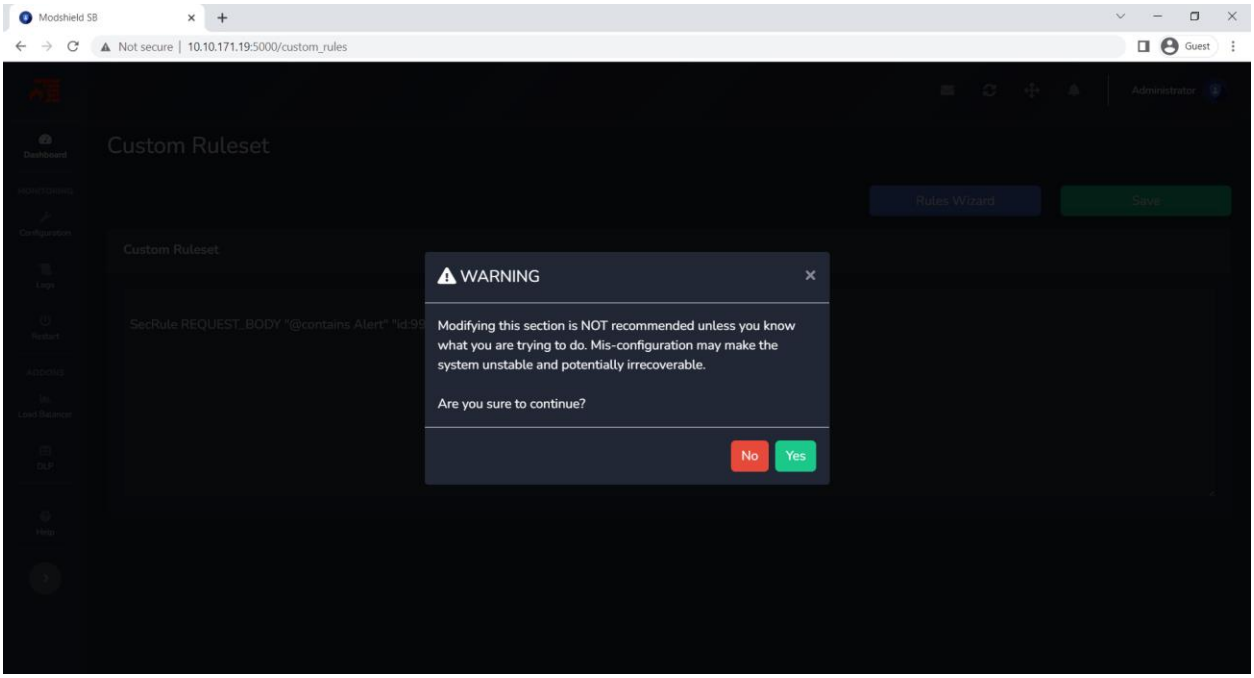
Click on Add rule



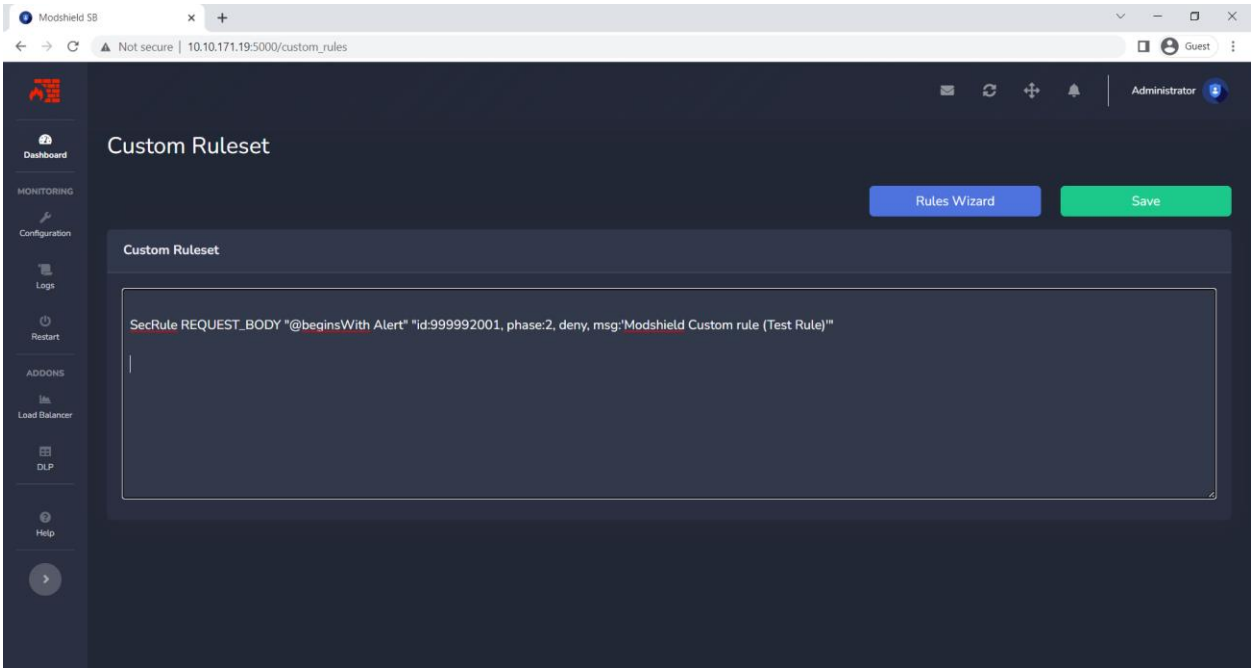
You will see the rule displayed in this text box. You can modify the rule here and hit save.



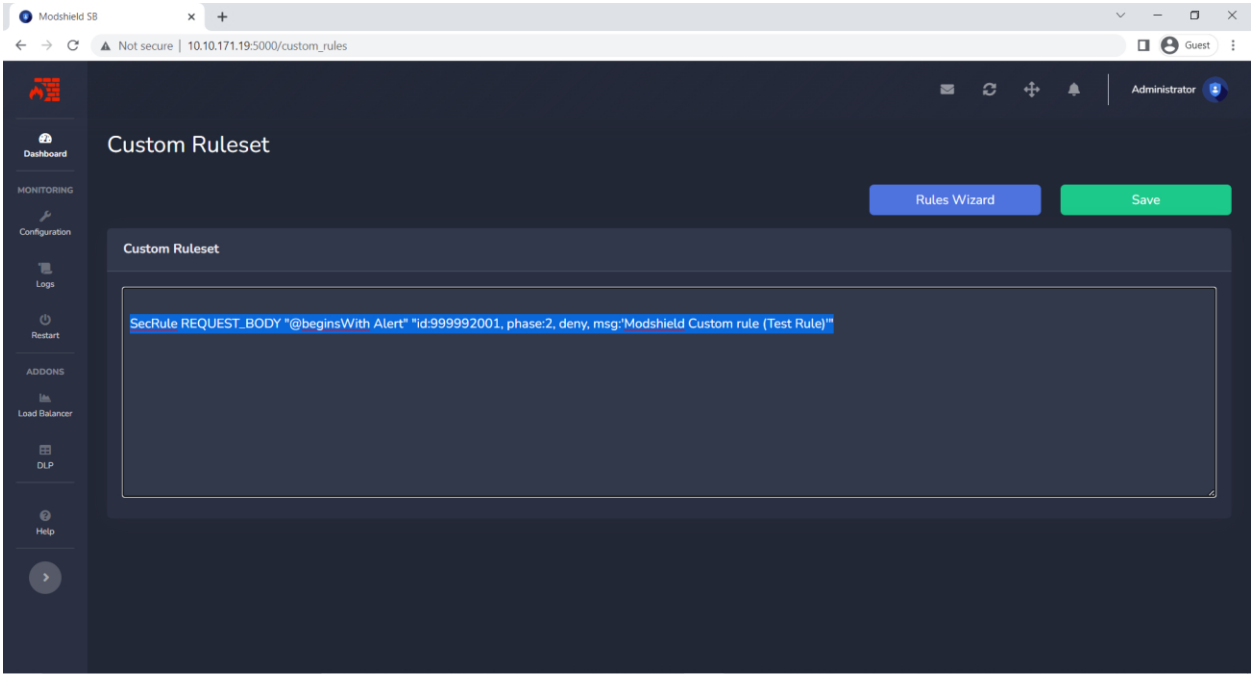
Mistakes in the custom rule can adversely affect the working of the firewall.



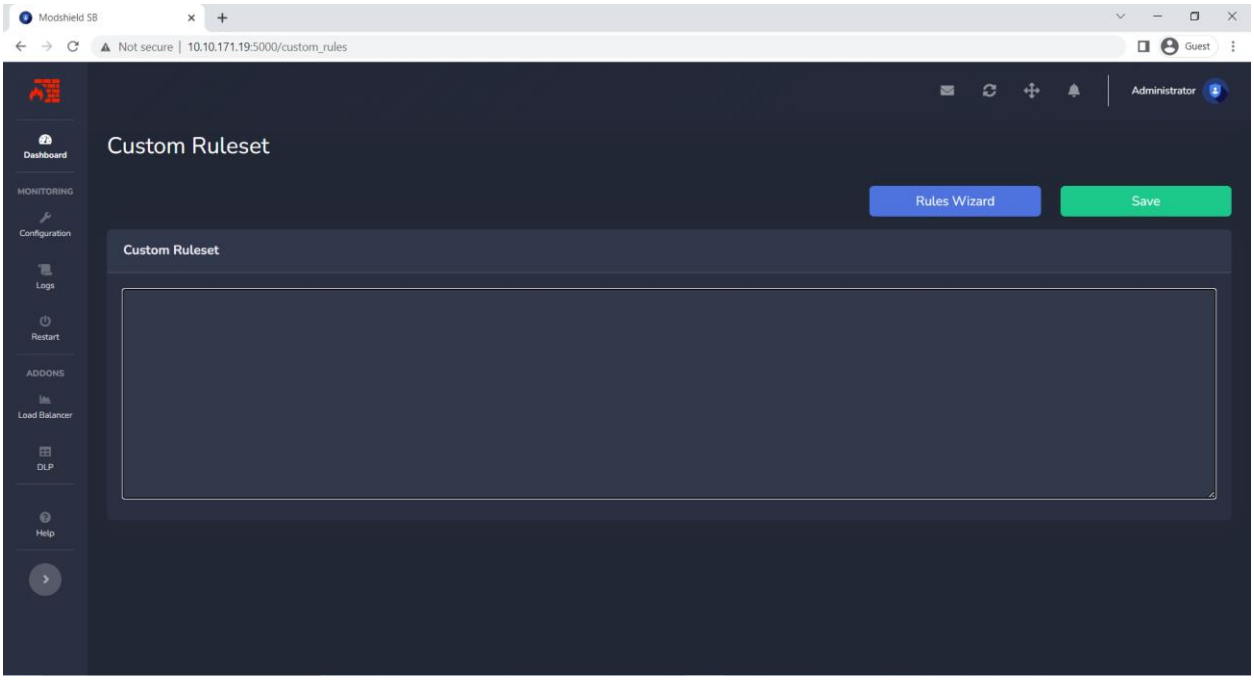
You can also write your custom rule here directly instead of using the wizard.



To remove a custom rule, select the rule and delete it. Save Changes



This will remove the custom rule from the firewall.

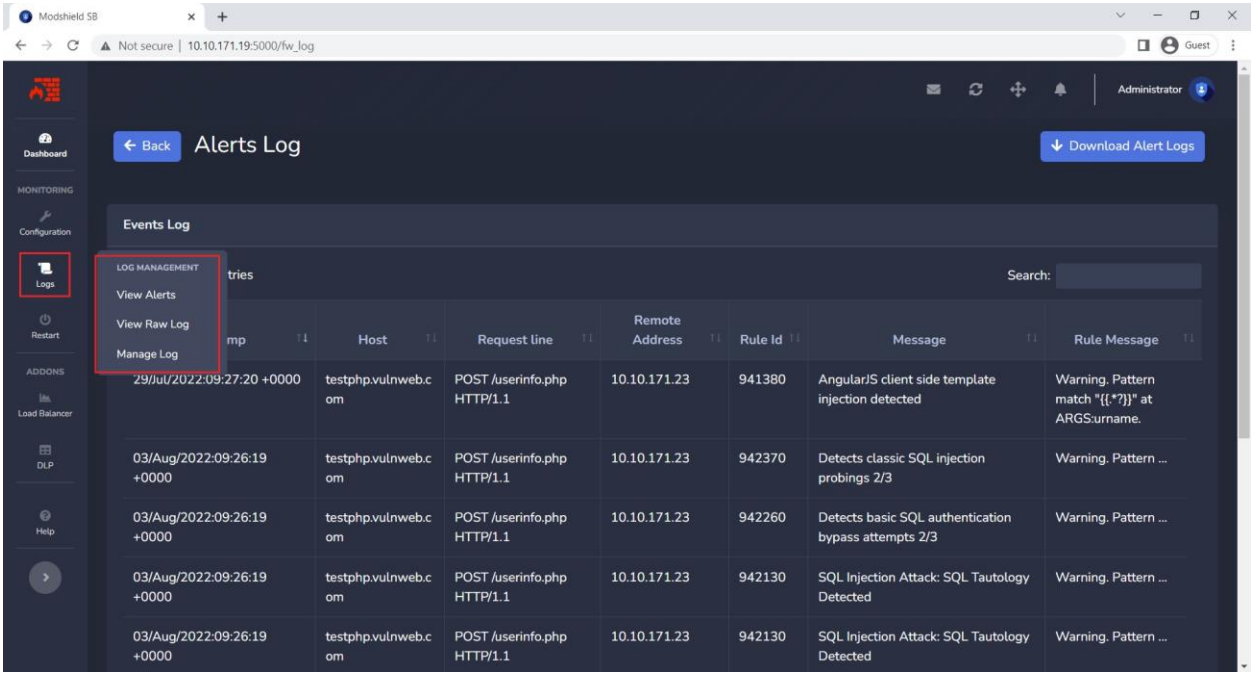


You can create as many custom rules as you need

Log Management

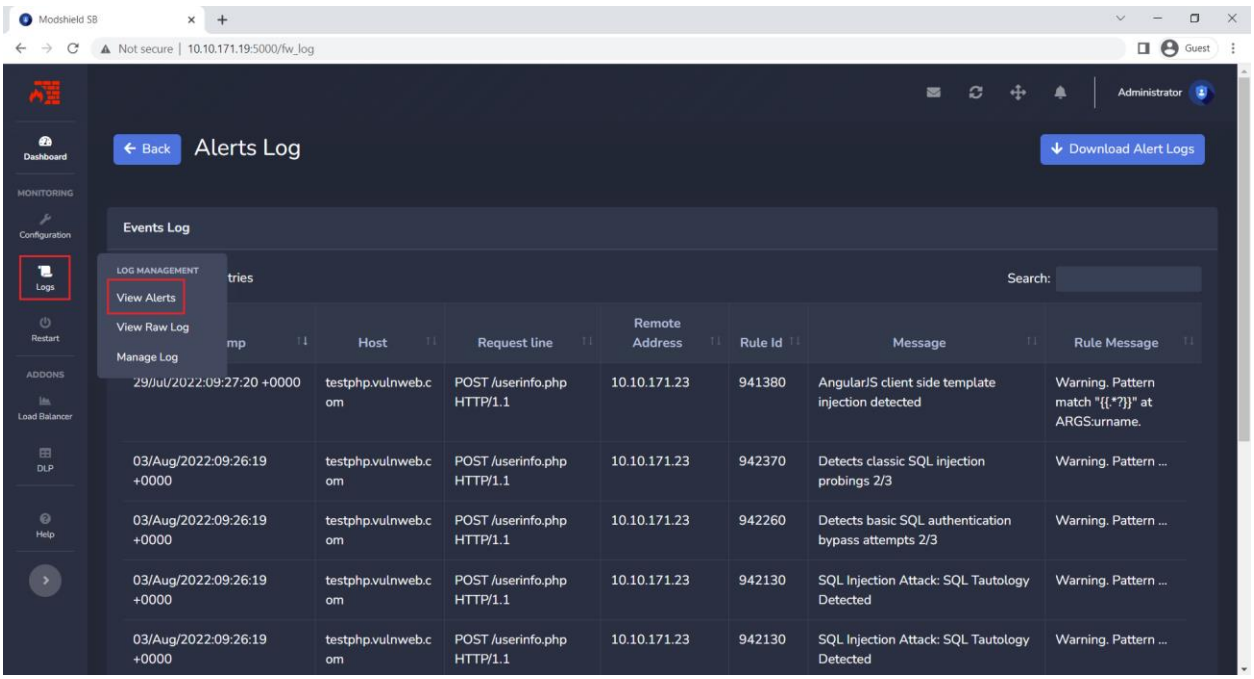
Video Link: https://youtu.be/TxLWpckvIuo

Modshield makes it very easy to analyze events and whole log files written by the firewall

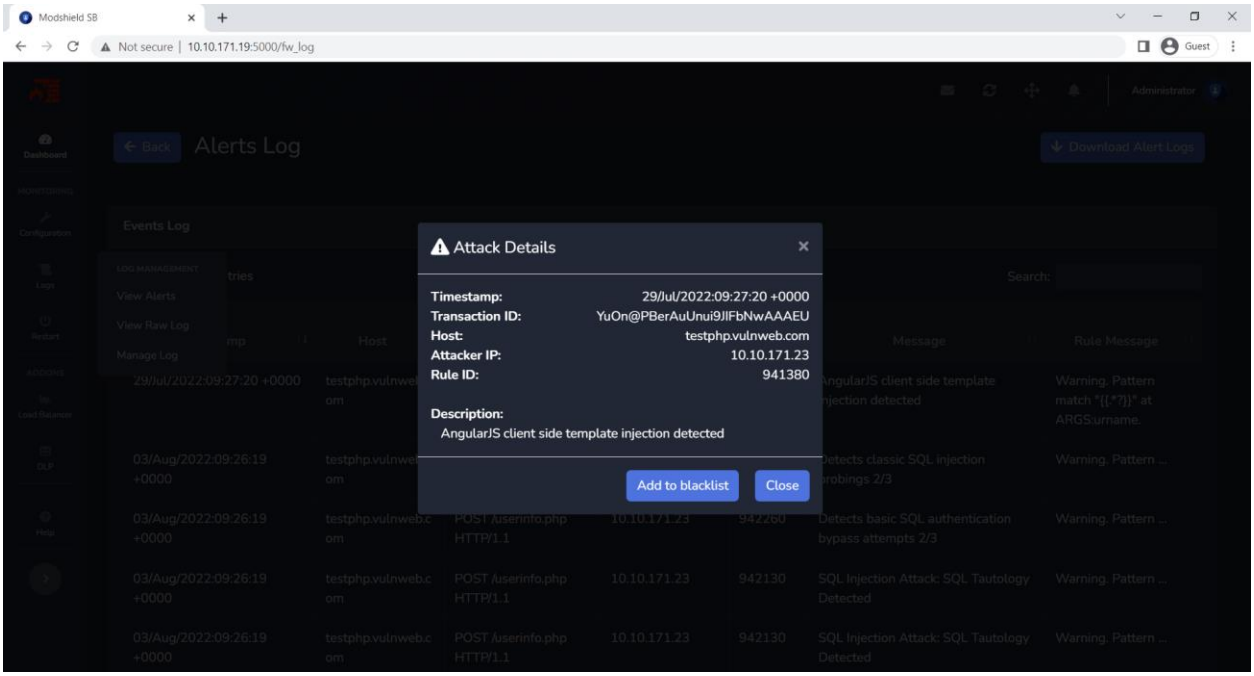


View Alerts

Click on View alerts from the Logs menu. This gives you a list of all threats blocked by Modshield

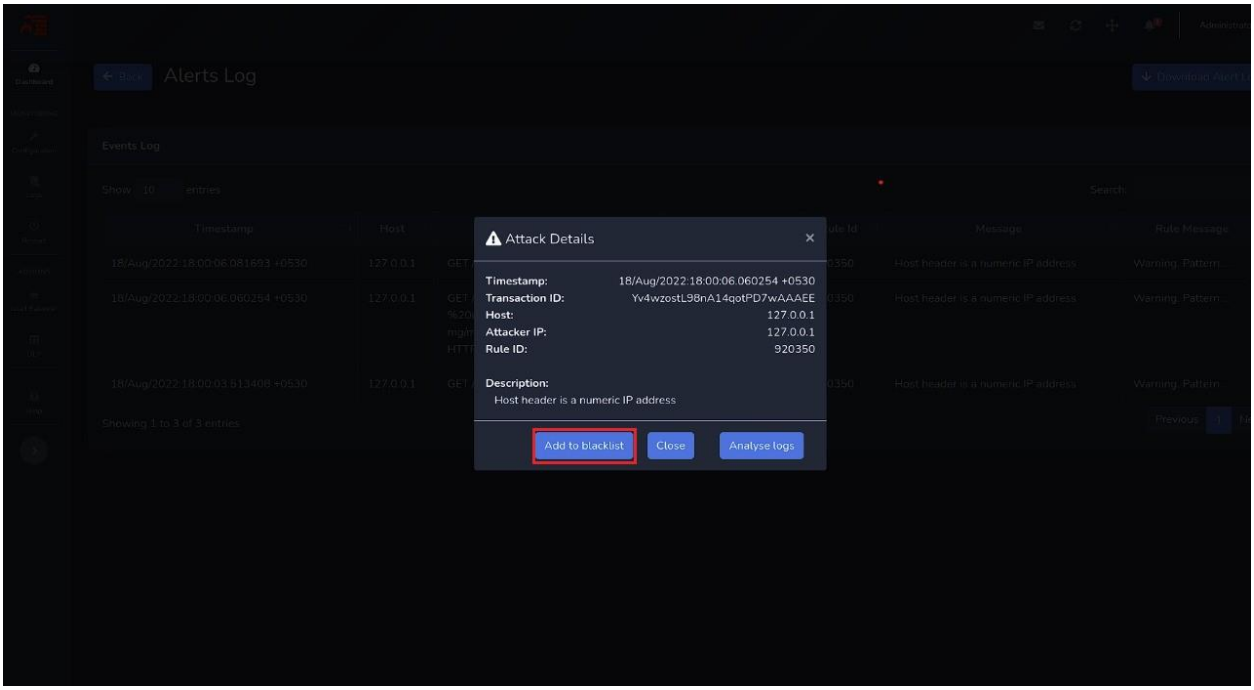


Click on any event line to see more details of the event



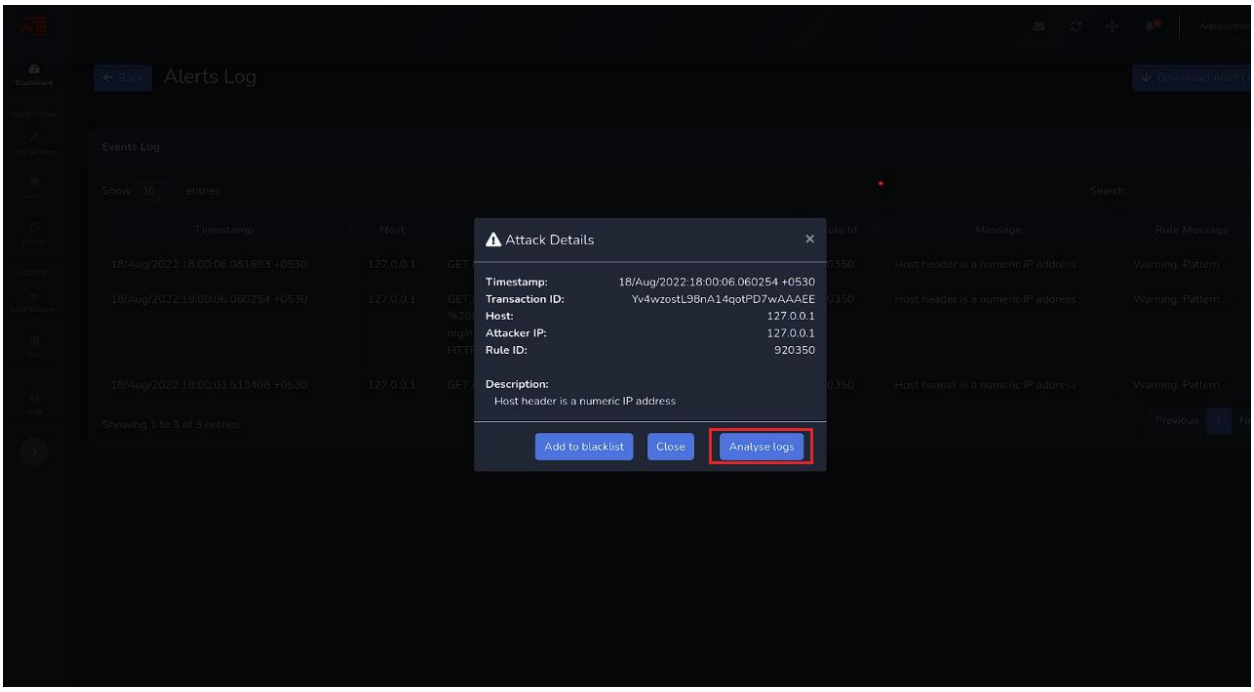
Blacklist IP

To blacklist the IP that is shown in the event, simply click the respective row, in “Attack details” you can see the “Add to Blacklist”

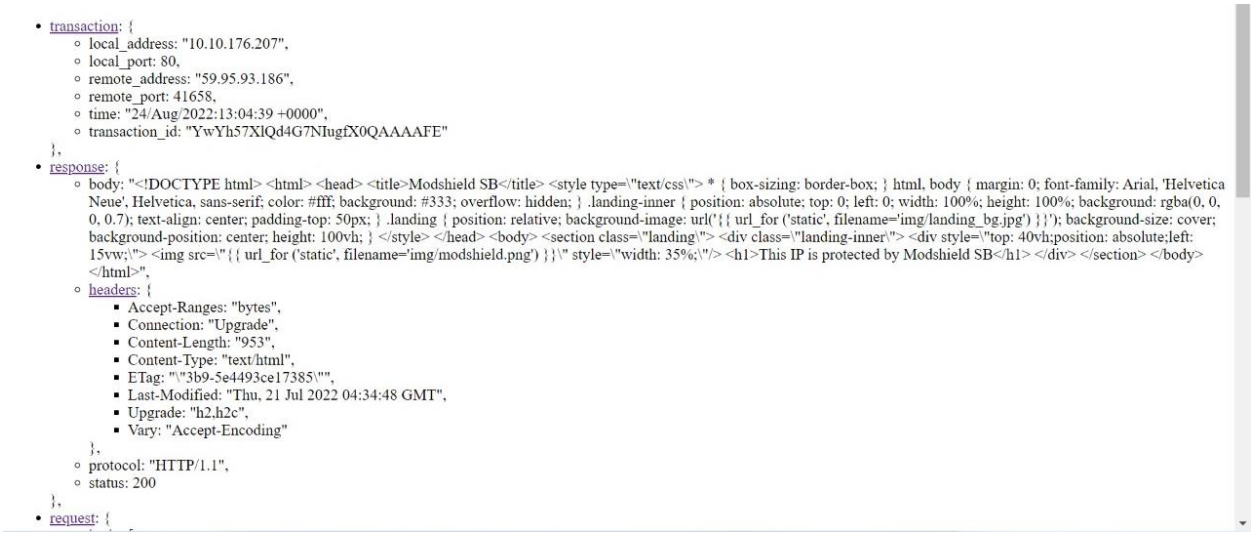


Analyse Logs

To deeply analyse the event, you can simply click "Analyse logs" in the attack details of the respective event in the Alert Logs.

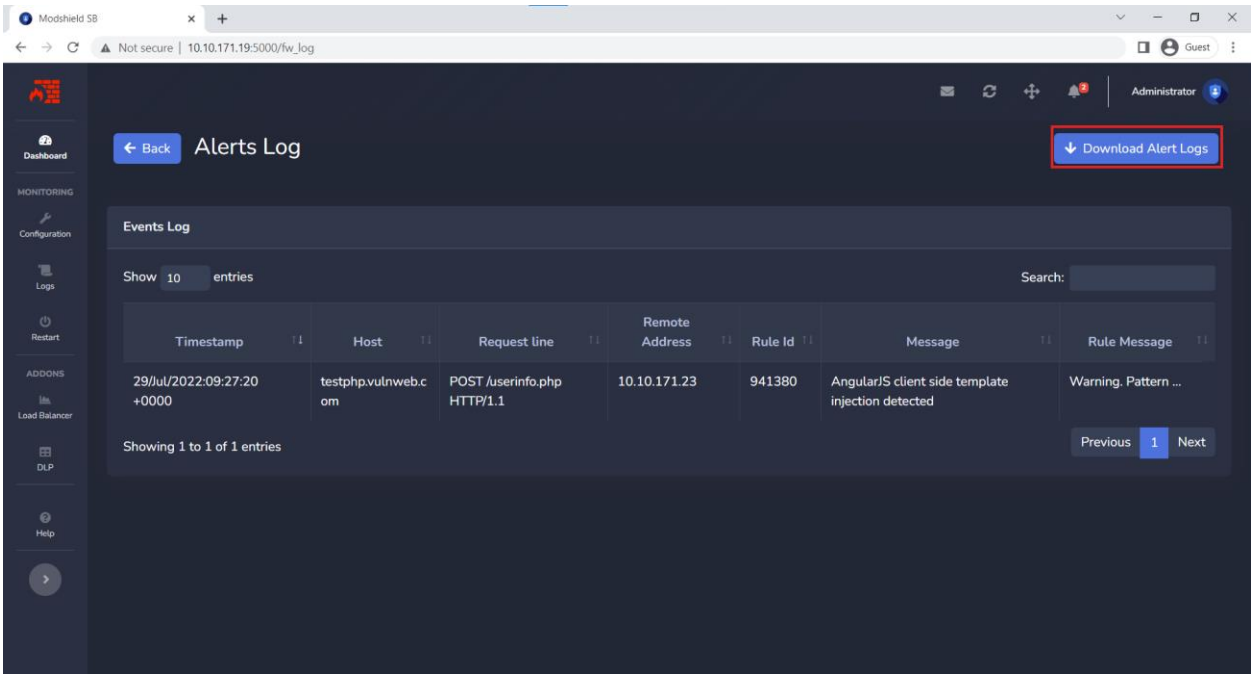


After clicking the “Analyse Logs” you will be seeing the structured and categorized event log in a new tab



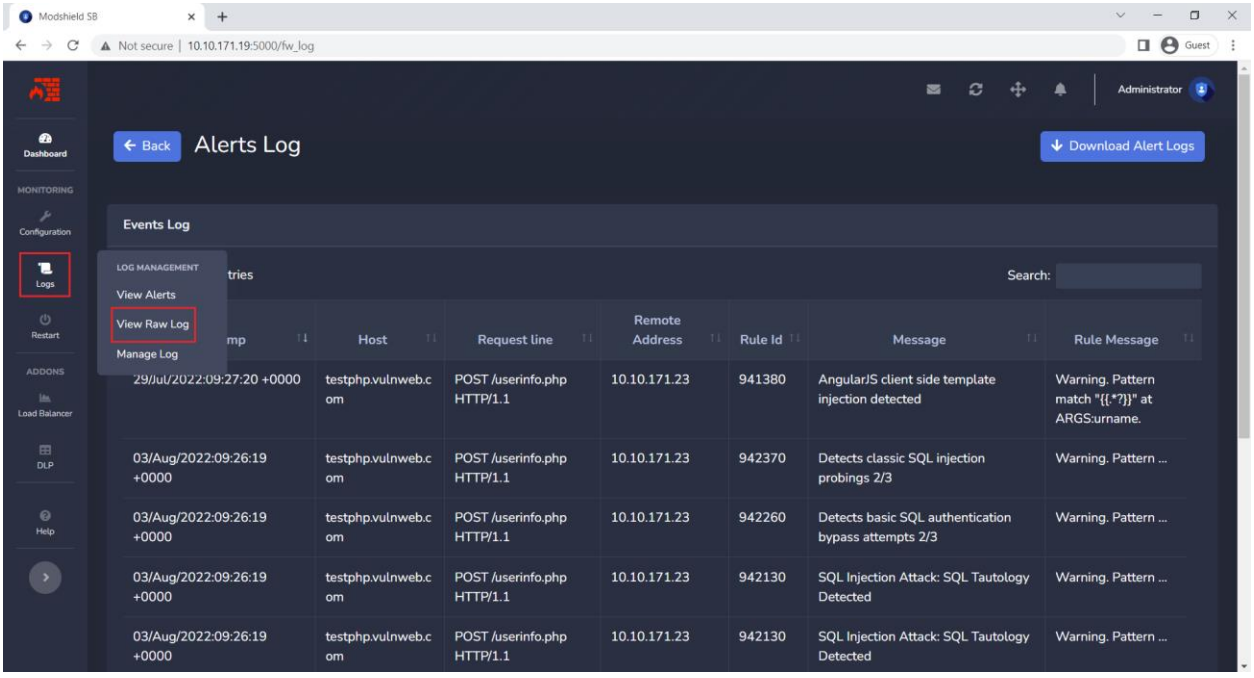
Download Alert Logs

You can download “Alert Logs” simply clicking the “Download Alert Logs” button at the top right side of the page. You can choose to store it in any location locally

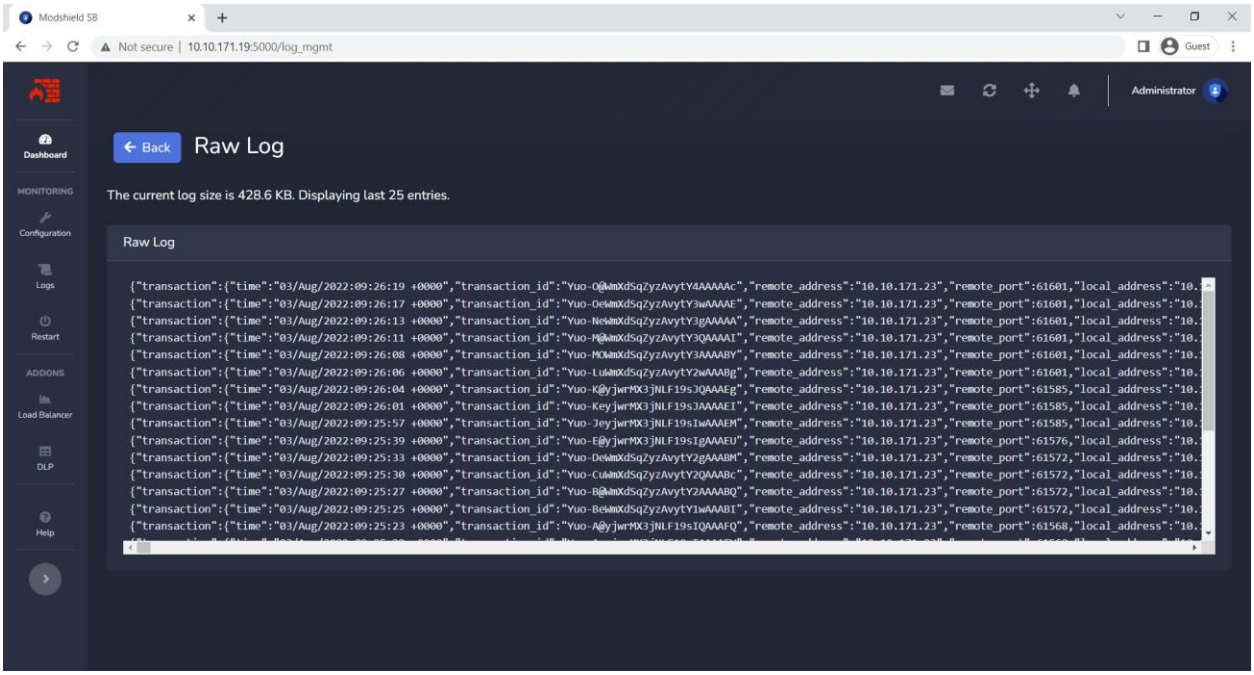


View Raw Logs

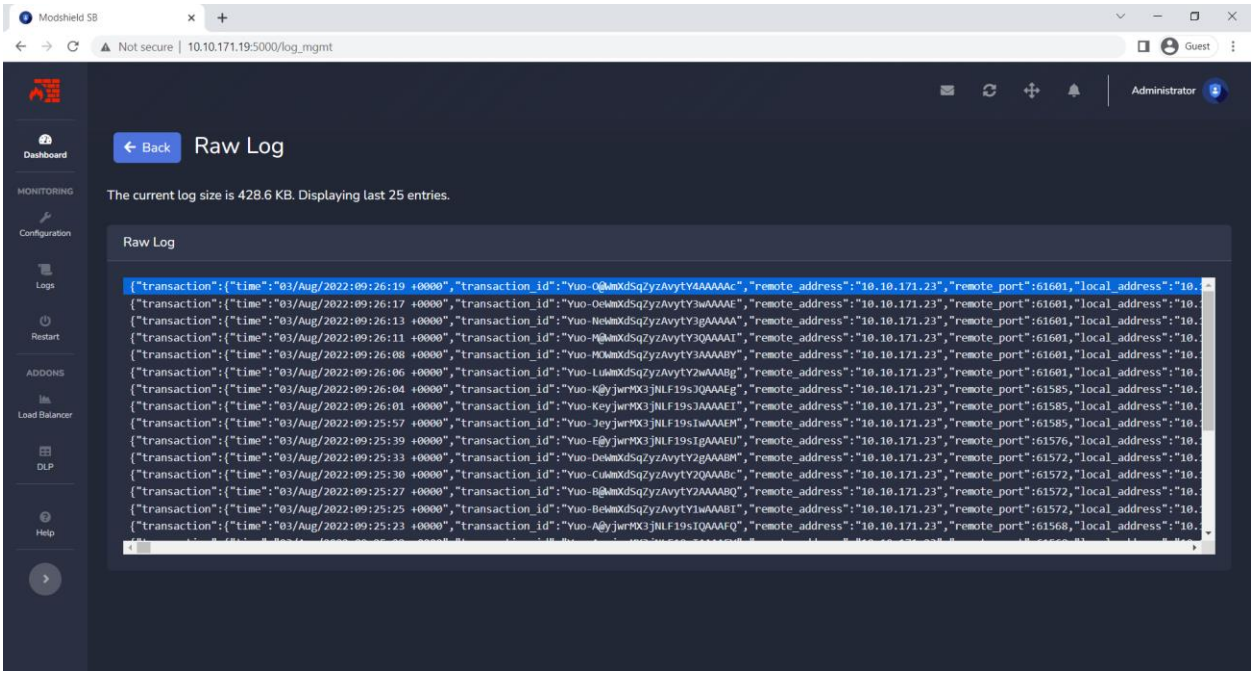
Modshield also provides an easy interface to view the associated raw logs. Select View Raw Logs from the Log Menu



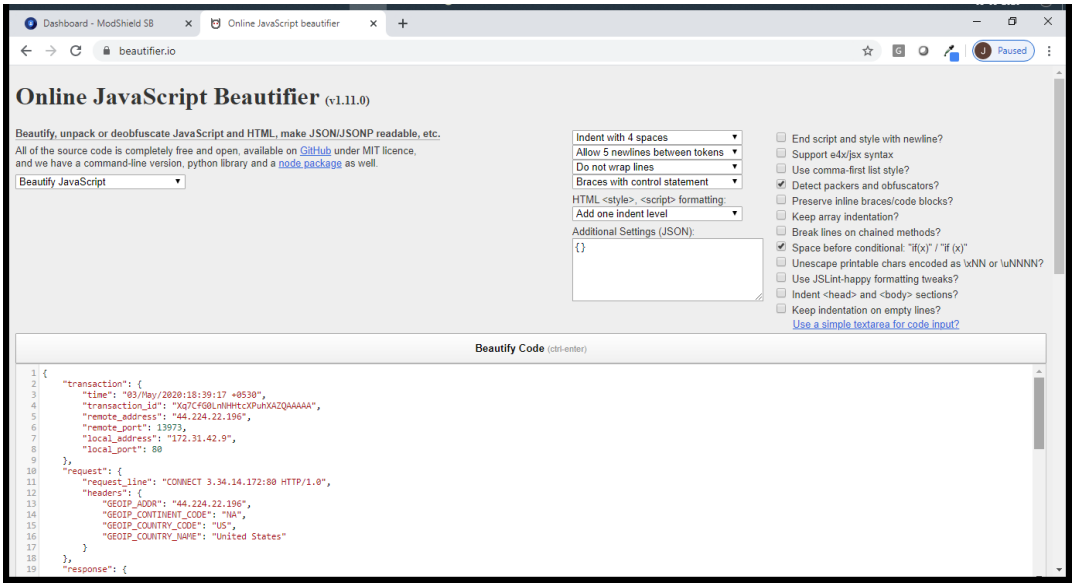
This lists all the log entries. The entries are in JSON format.



You can copy an entry that you are interested in, and beautify it using any tool

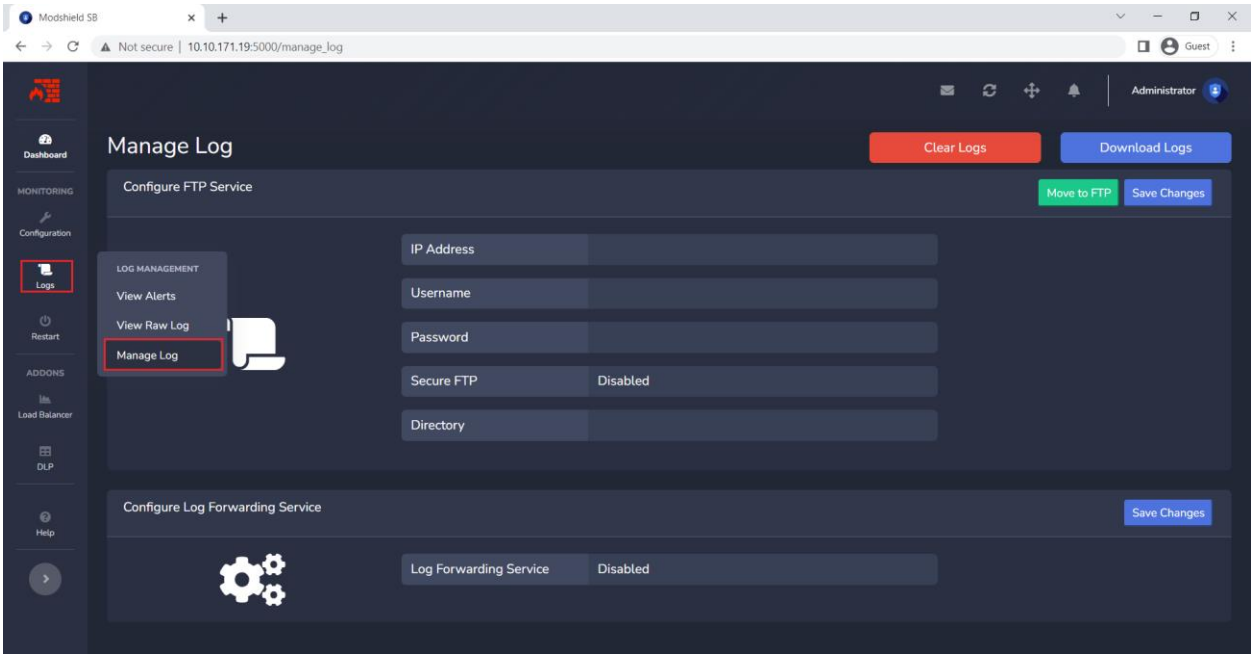


I use beautifier.io to render the log entry in a readable JSON format. When you forward logs to an external listener, this is the format that you will be parsing

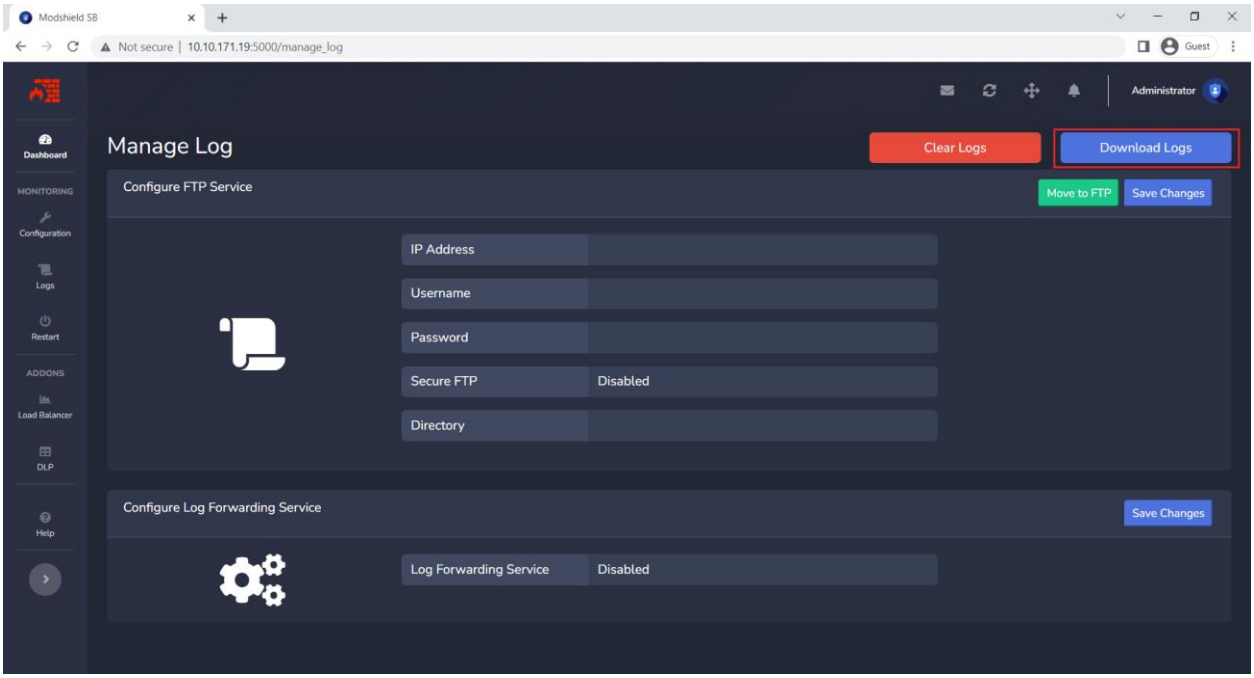


Download Raw Logs

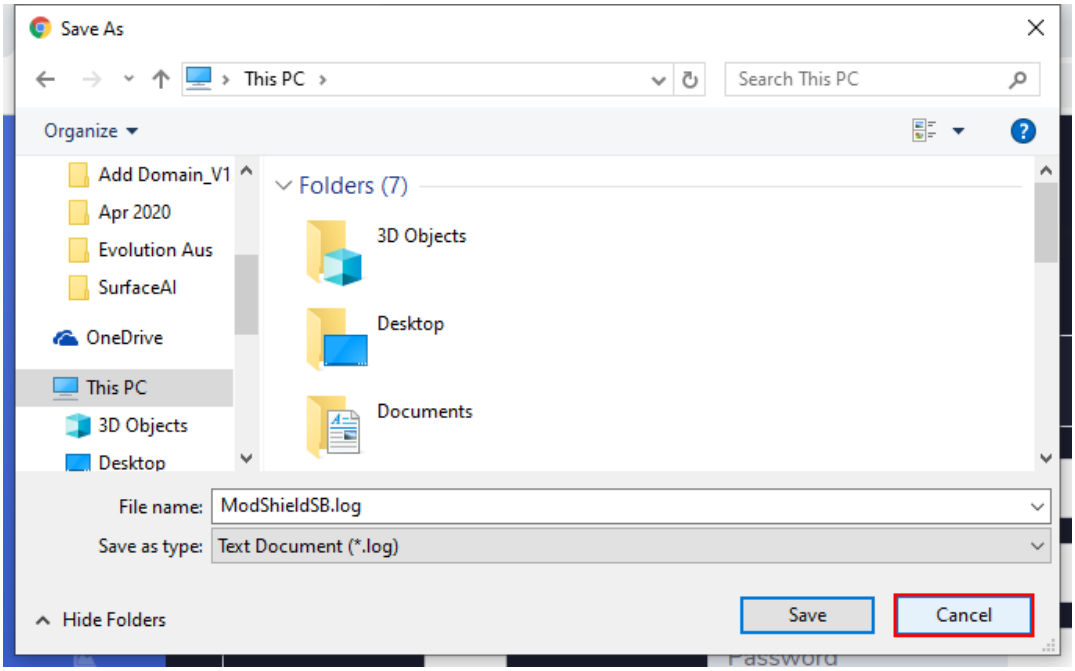
Log files need to be managed, archived or transferred. This can be done using the Manage Log Option



The Download Log button allows you to download a copy of the log file, locally

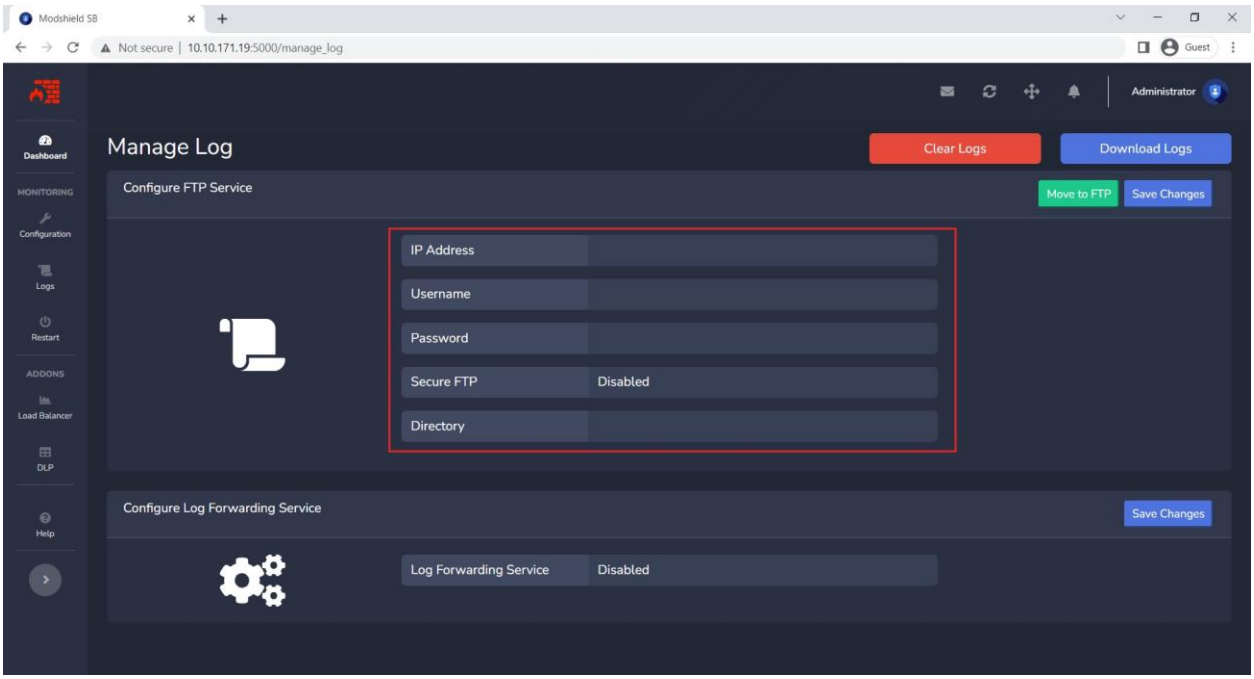


You can choose to store it in any location locally

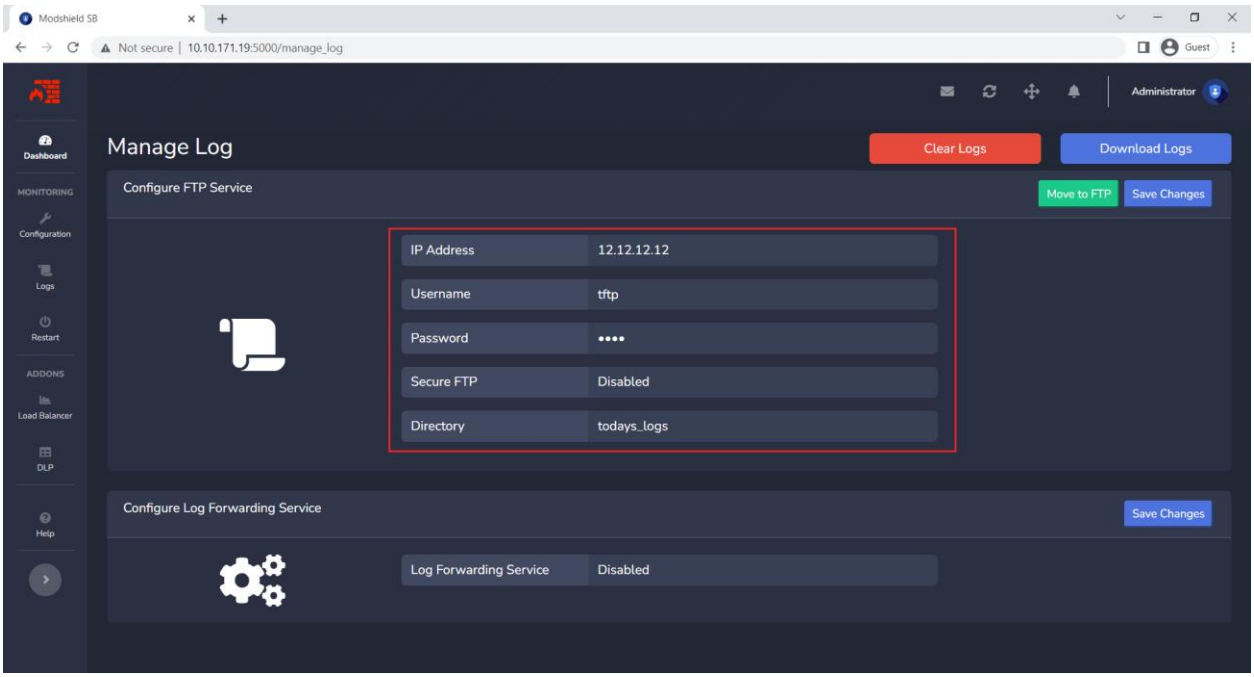


Transfer Logs using FTP

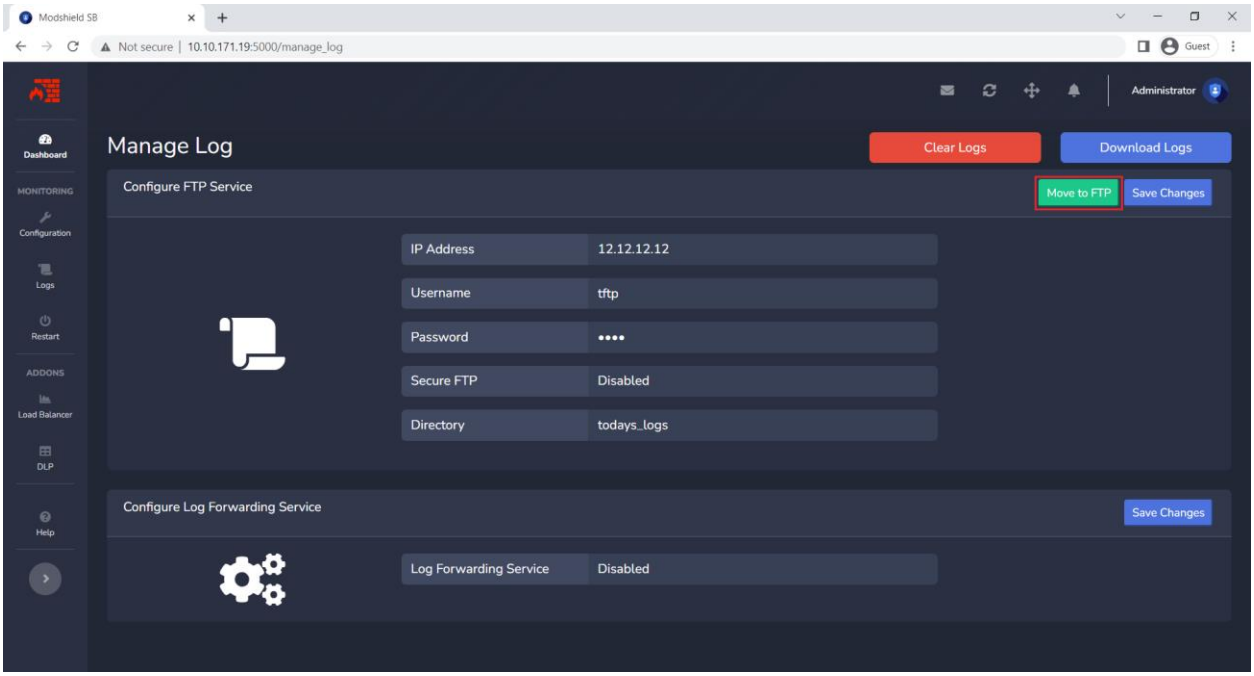
You can also transfer the log files using FTP



Simply configure the FTP details and the directory to which the log files are to be transferred. You can enable secure FTP if it is allowed for your transfer

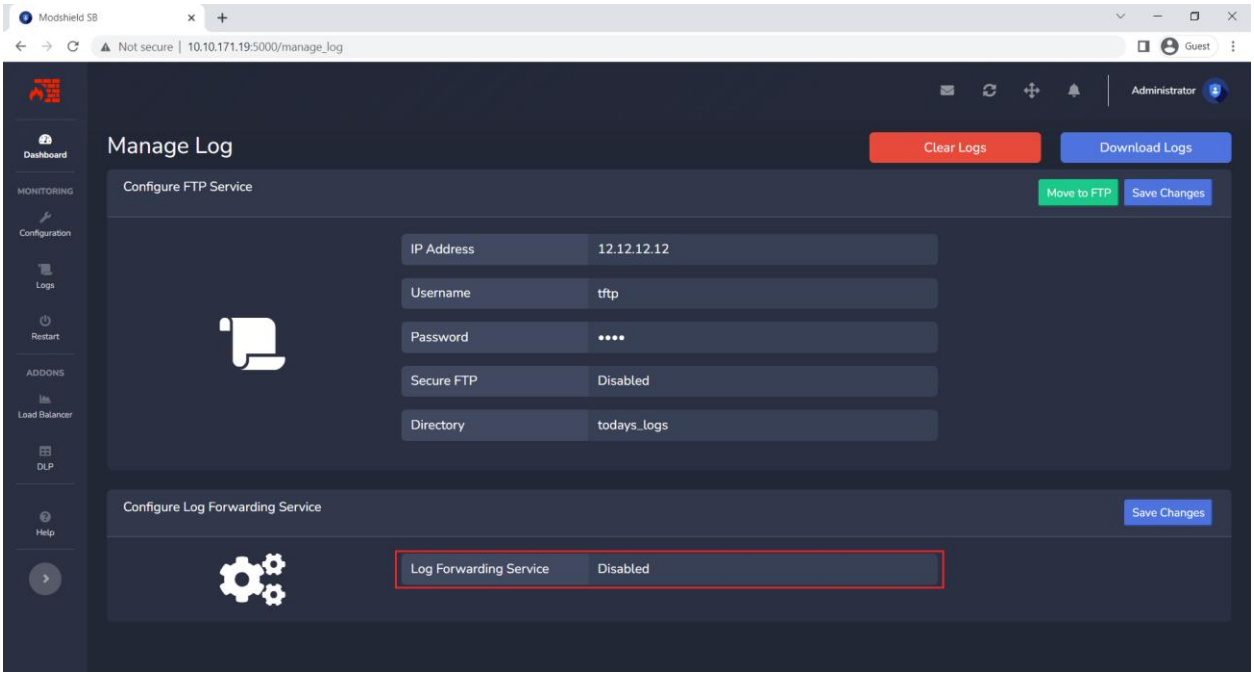


Once configured, click on "Move to FTP" to move the log file. Once moved, the log files will be cleared in the firewall and the dashboards refreshed

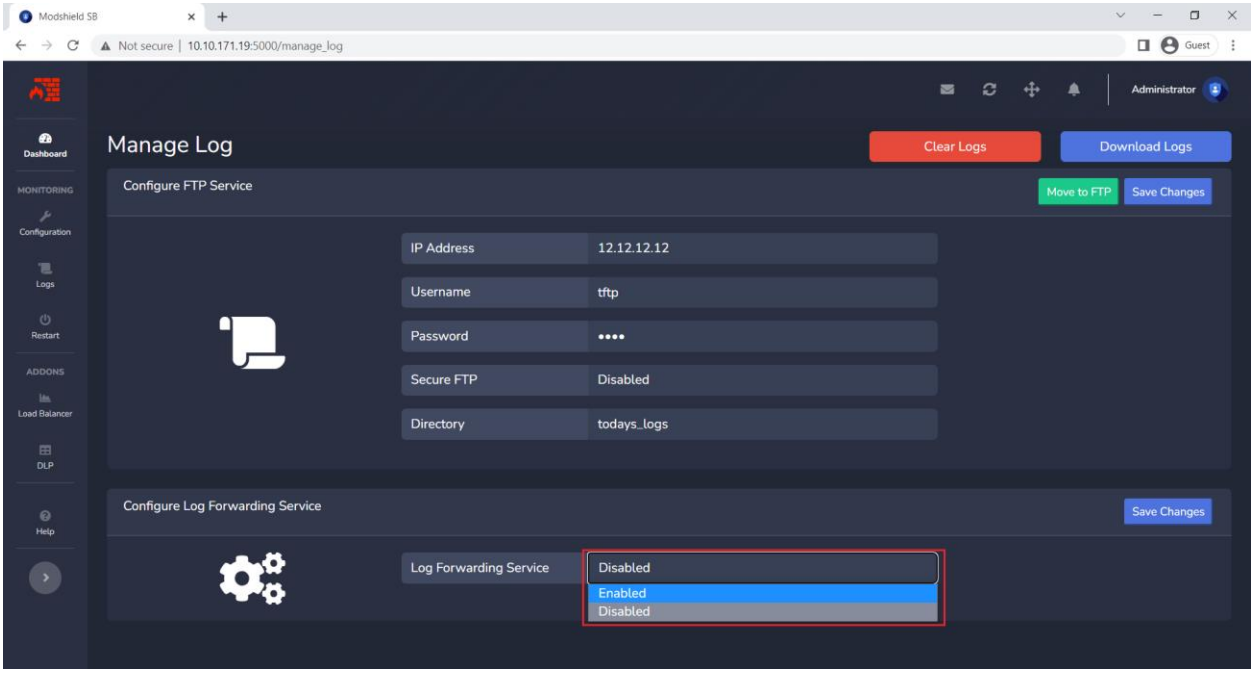


Log Forwarding

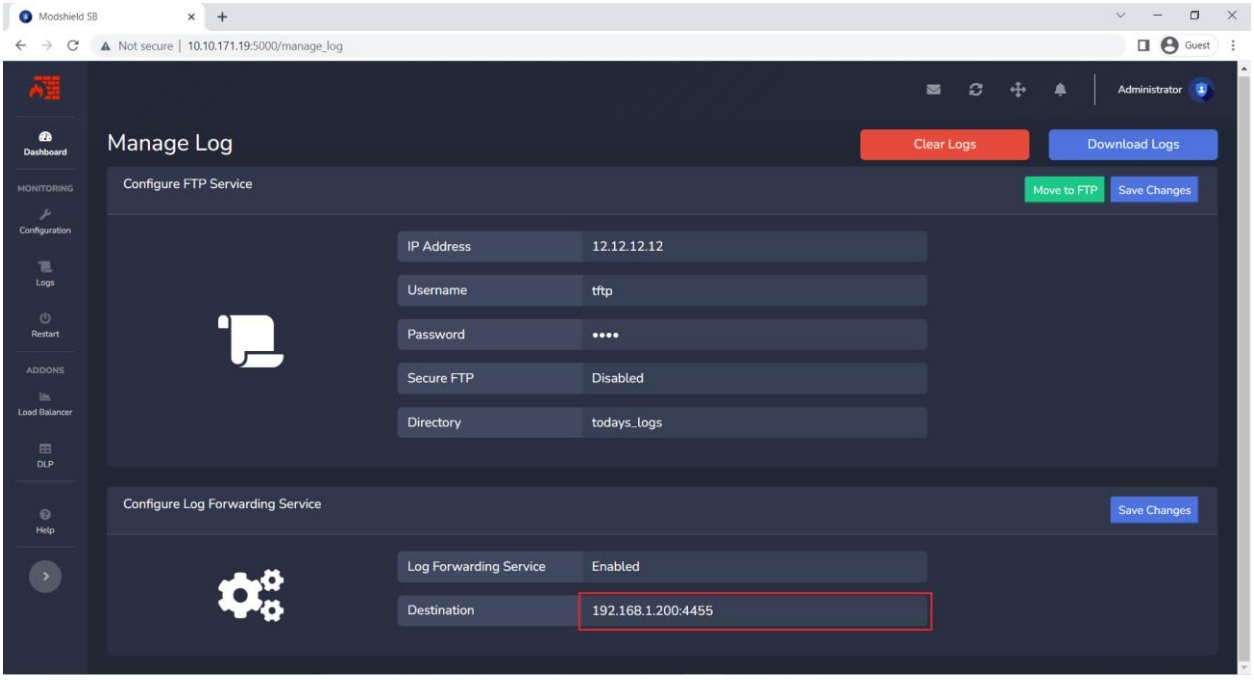
You can enable real time log forwarding to an external listener service



Enable this service to forward every log entry as it is written to the log file



Enter the IP address and the port details of the listener and Save Changes



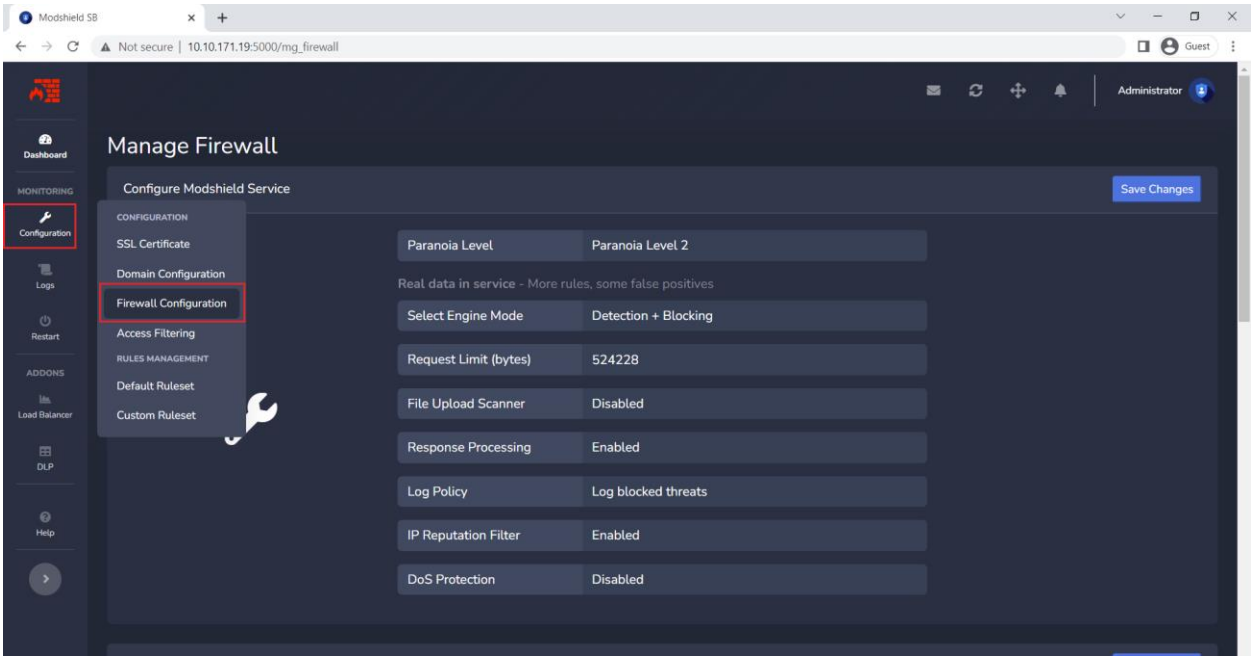
The forwarded messages will be in the same JSON format as in the raw logs.

Update Modshield

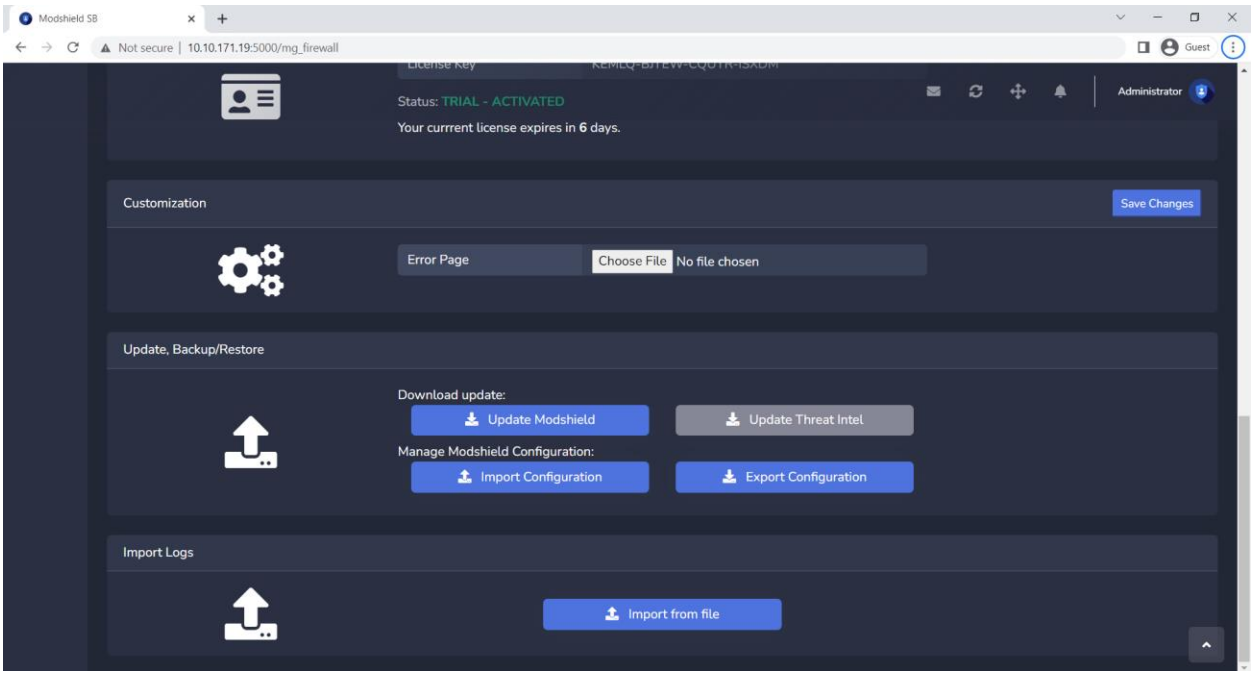
Video Link: https://youtu.be/OpNaGKcRpHI

Modshield is constantly kept current through updates that are published regularly

To update Modshield, scroll down to the update section in Firewall configuration

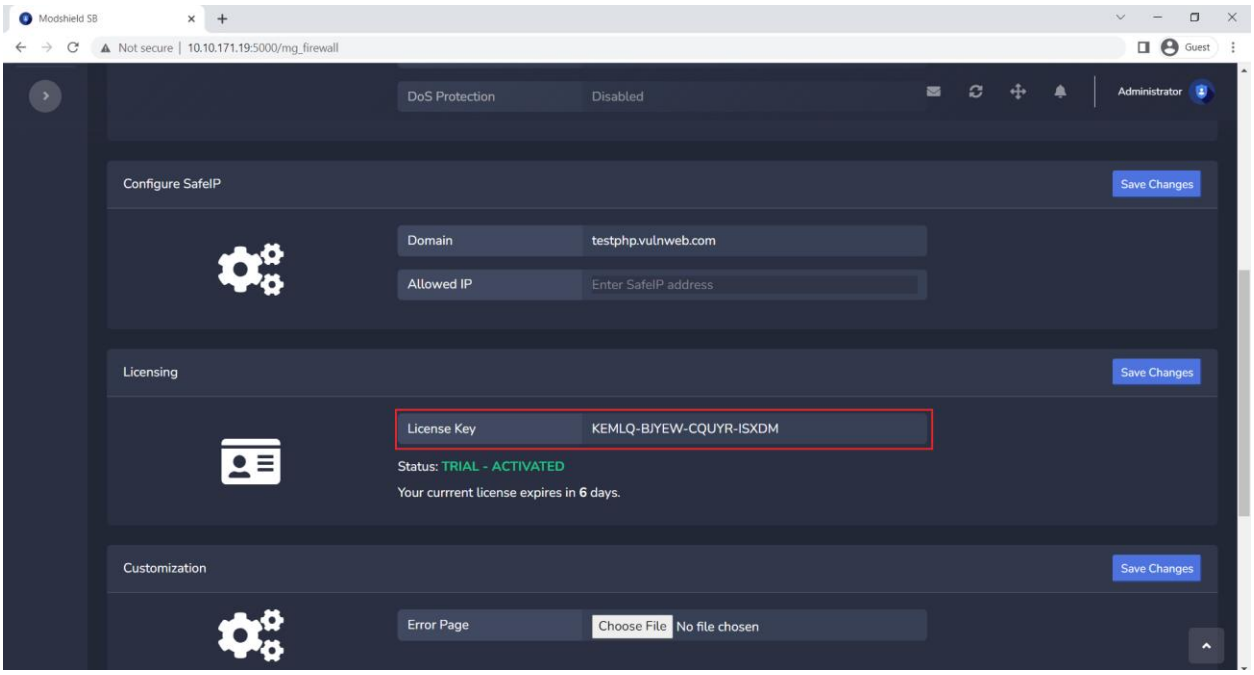


Threat intelligence, rules, software and the Geo IP data updates are made available



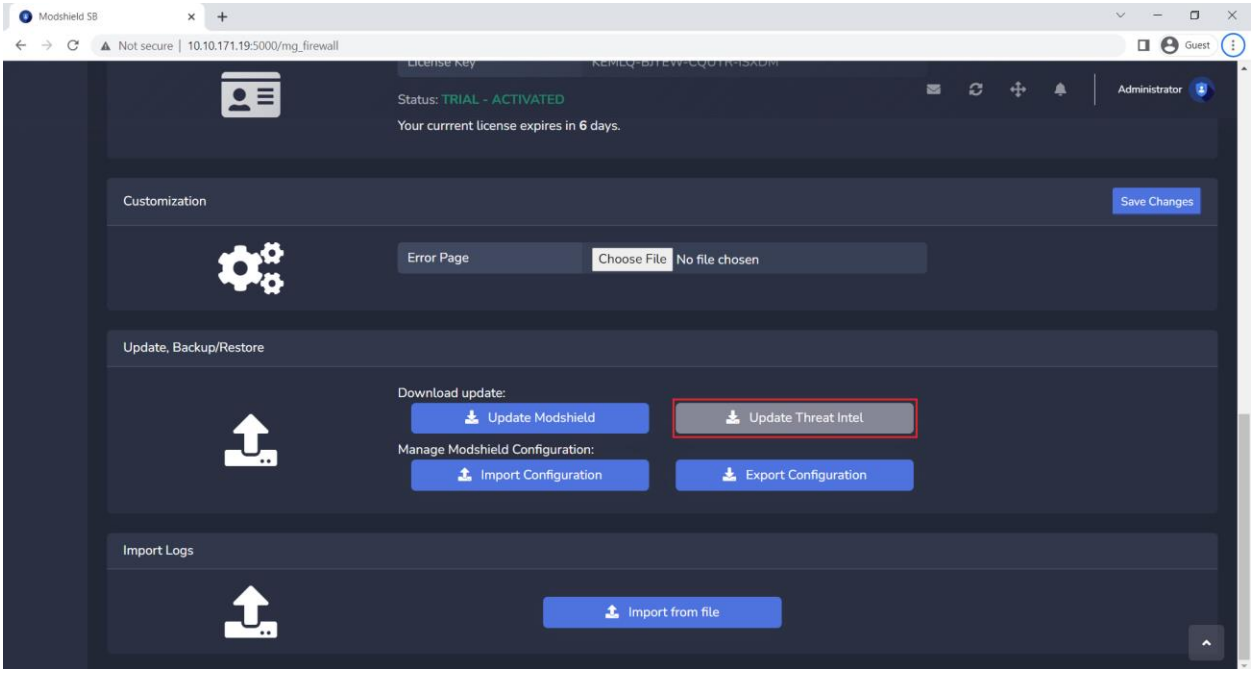
Update License

You can also update any changes in your license information using this screen



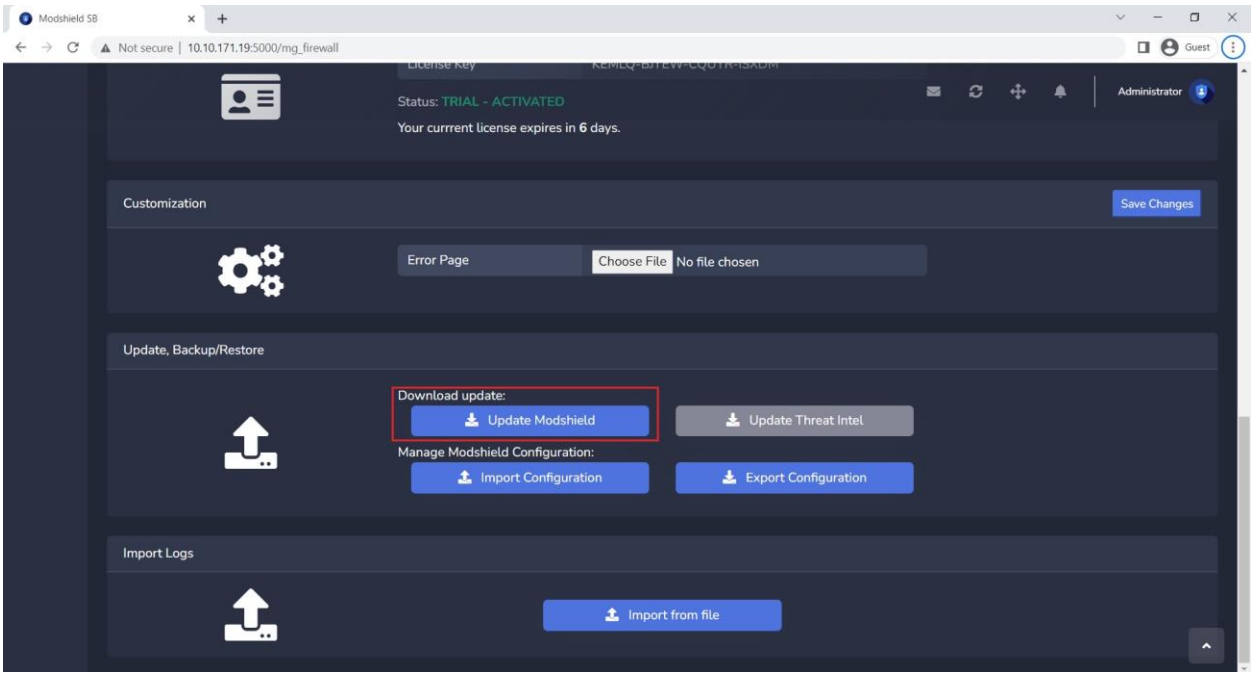
Update Threat Intelligence Feeds

Threat Intel provides Modshield with information to identify bots, crawlers, bad IPs and so on



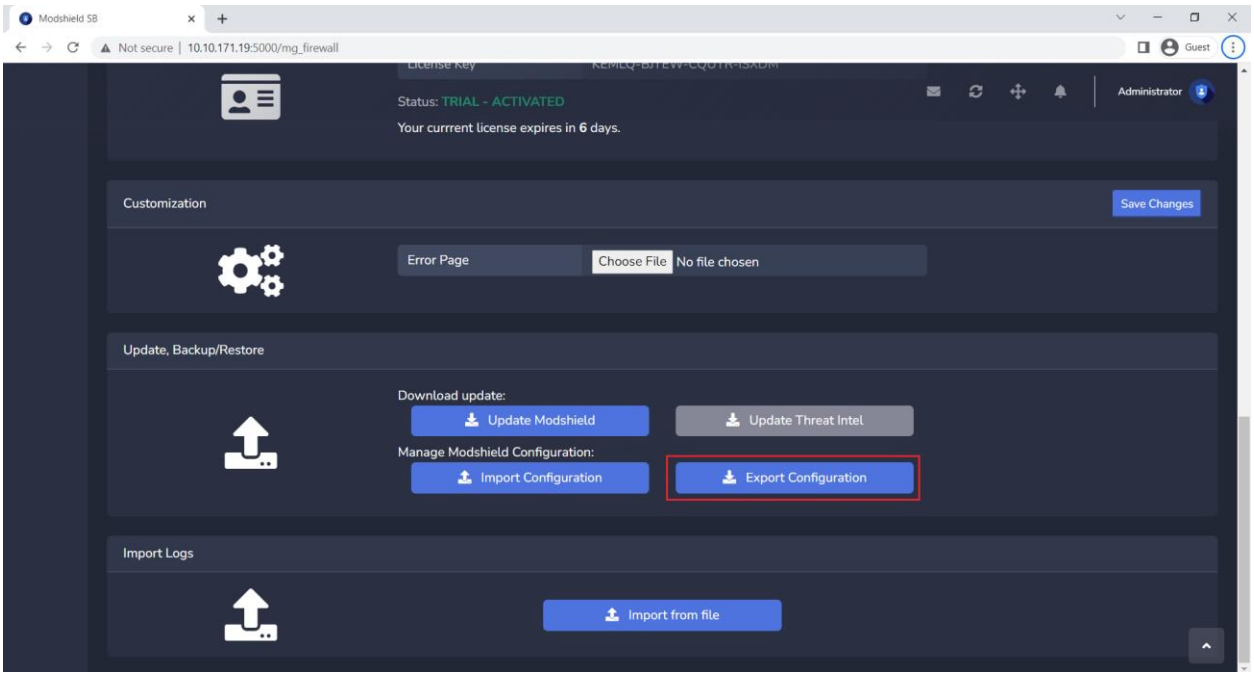
Modshield Updates

Modshield upgrades help us push rules and software updates to all instances

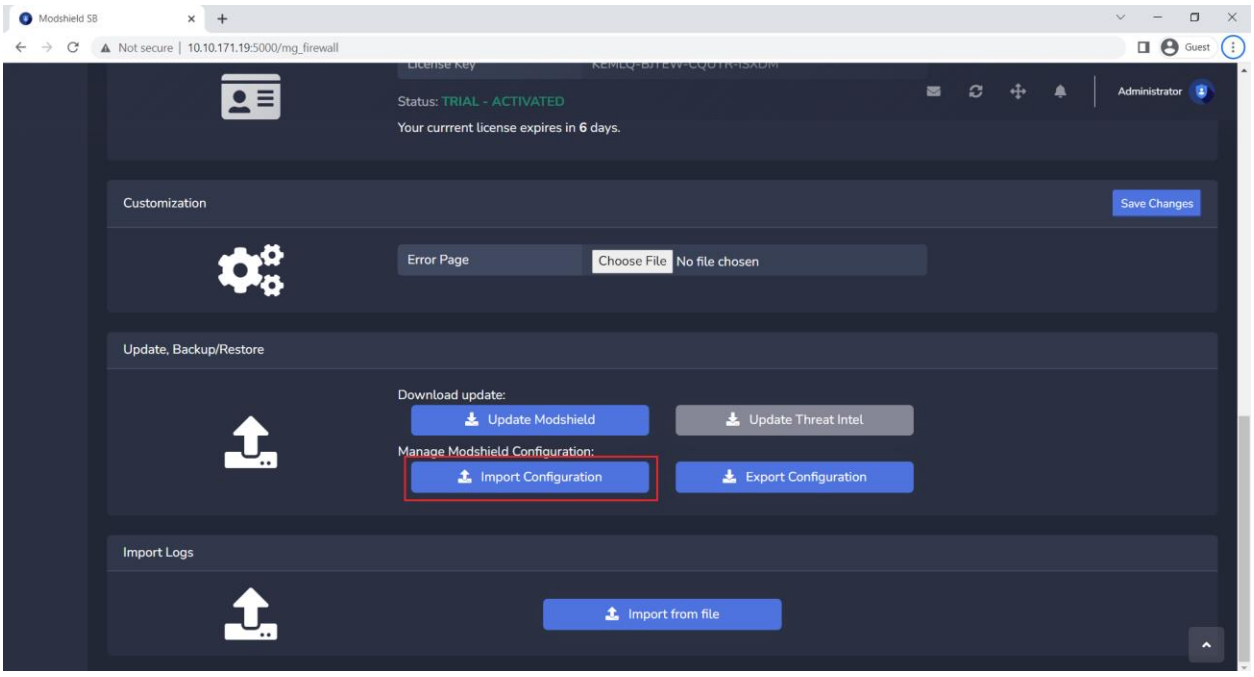


Import / Export Configuration

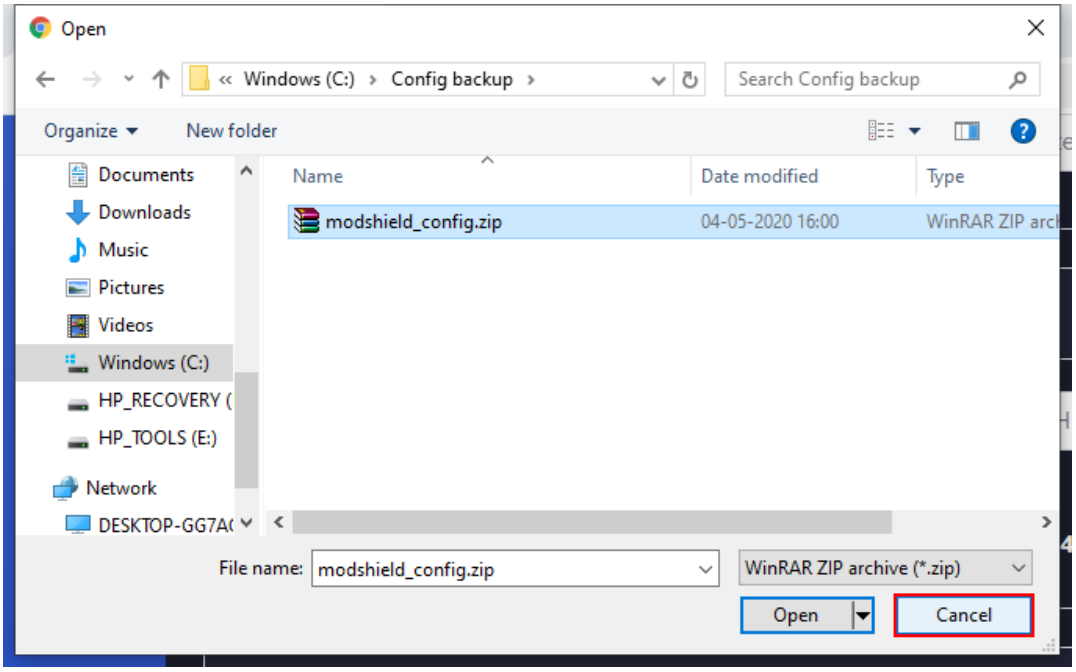
To back up the firewall configuration, you can export the configuration and store it locally



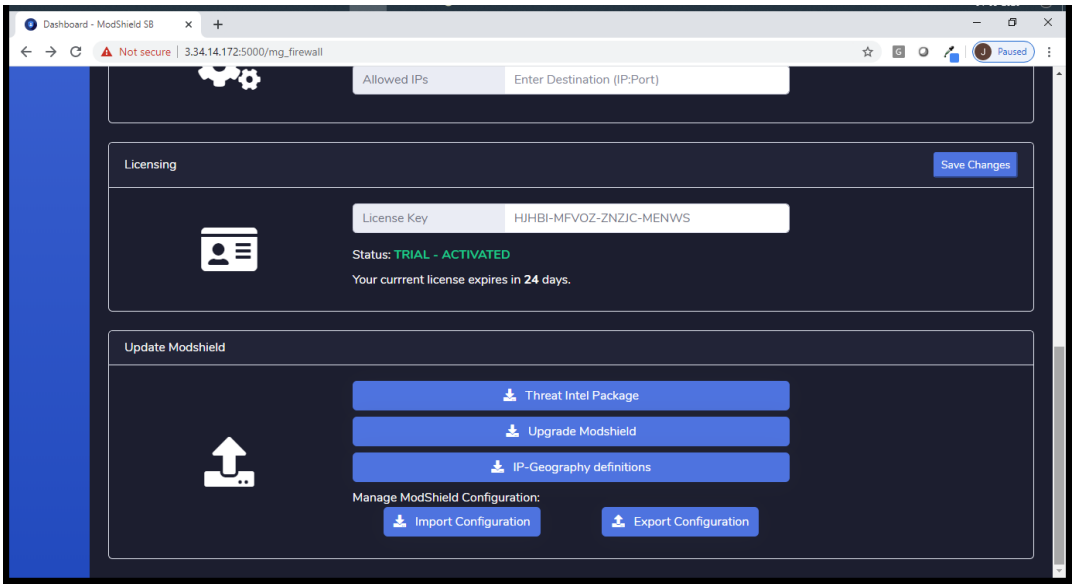
You can also use that to import the configuration into another firewall instance



This is very useful if you are managing multiple firewalls and would like to replicate the settings. This also allows you to import custom rules, DLP settings etc. from another firewall



We encourage you to keep your firewall instance updated regularly using these options



References

Certain definitions from OWASP, SANS and Wikipedia have been referred to in the creation of this document