

Advance DDOS Explained:

With this new addition there will 2 kinds of DDOS protection option available to all sites.

- Basic DDOS Protection**
 This is a rate limiting rule, which will limit the number of requests an IP can make to a website in 2 minutes
- Advance DDOS Protection**
 This is advance rate limiting rule, which will limit the number of requests a user can make to a website in 2 minutes. This is done using advance fingerprinting.

The feature is made extremely user friendly and customer can control the thresholds and choose to enable or disable the role from portal.

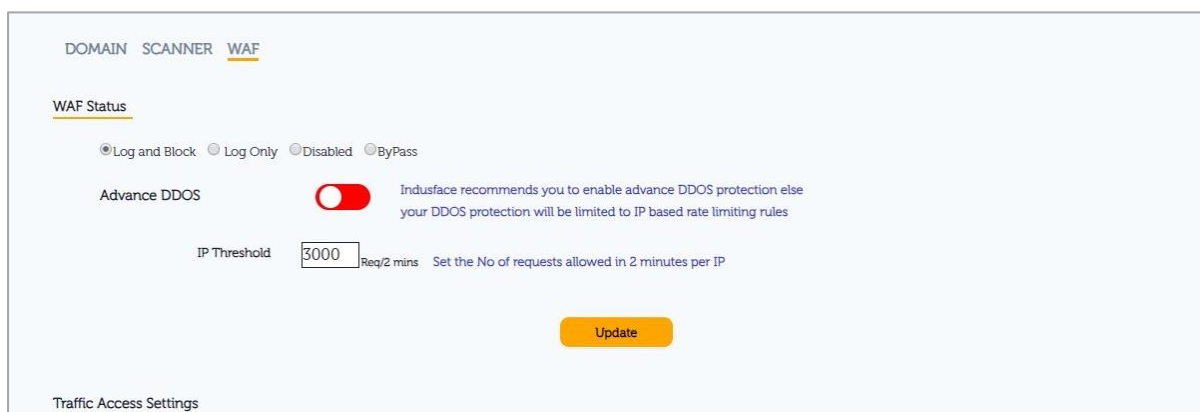
The workflow will be as follows-

By default, all websites will be placed on Basic DDOS Protection. This means IP based rate limiting rules are applied to all websites. The rate limiting is governed by the IP Threshold value. By default, it is set to 3000 req/2 min.

This means, if from a same IP the website receives more than 3000 req in 2 mins then the IP will be marked malicious and any further traffic from the IP will be blocked.

Once the IP is marked malicious, AppTrana would require 3 mins of cool down period before it allows the request from the same IP. i.e.) For a period of 3 minutes, AppTrana should not receive any further request from the malicious IP. If it continuous to receive requests from the IP, then it will continue to block until there is a cool down of 3 mins where no request is received from the IP.

The threshold value can be changed by customer from the portal.



The screenshot shows the 'WAF' configuration page. At the top, there are tabs for 'DOMAIN', 'SCANNER', and 'WAF'. Below the tabs, the 'WAF Status' section has four radio buttons: 'Log and Block' (selected), 'Log Only', 'Disabled', and 'ByPass'. The 'Advance DDOS' section features a red toggle switch that is currently turned on. To the right of the toggle, a message reads: 'Indusface recommends you to enable advance DDOS protection else your DDOS protection will be limited to IP based rate limiting rules'. Below this, the 'IP Threshold' is set to '3000' in a text input field, with 'Req/2 mins' and the instruction 'Set the No of requests allowed in 2 minutes per IP' next to it. An orange 'Update' button is located at the bottom center. At the bottom left, there is a link for 'Traffic Access Settings'.

For disabling the rule, one should put extremely high value for the threshold i.e., 999999

Customers who already have rate limiting rule enabled for their site will have this rule's threshold value set according to their current value.

Advance DDOS

Basic DDOS works with IP as identity. In many cases, IP would not be enough. There could be many machines connecting from same IP and more granularity would be required. For this, AppTrana provides the option of Advance DDOS.

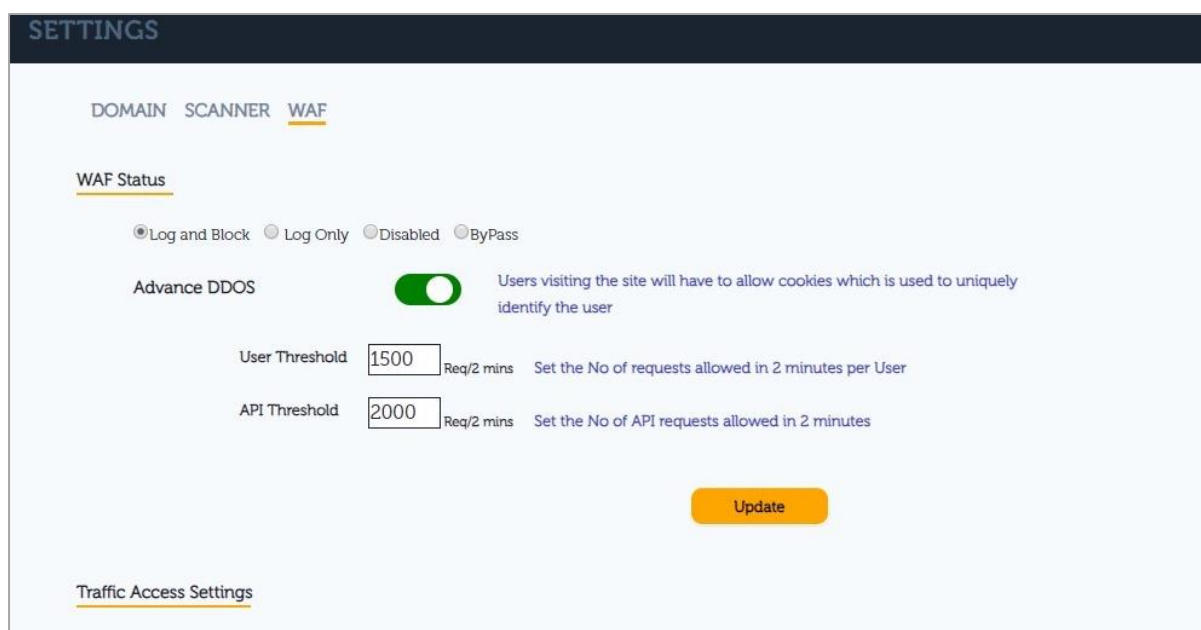
When Advance DDOS is enabled, users will be tracked with help of a cookie that would be injected when the user tries to connect to the website first time. This cookie is non-intrusive and no personal information are tracked using this cookie. This cookie creates a fingerprint to identify the user separately.

When Advance DDOS is enabled, 2 thresholds will be in play.

User Threshold – This governs the number of request a user is allowed to be made in 2 mins. Default value is 1500/2 min

API Threshold – API's won't be able to serve cookie, it is for this reason API traffics are isolated and they are tracked by IP. This threshold's number of requests the API server can make in 2 minutes.

Default value is 3000/ 2 min.



SETTINGS

DOMAIN SCANNER WAF

WAF Status

Log and Block Log Only Disabled ByPass

Advance DDOS Users visiting the site will have to allow cookies which is used to uniquely identify the user

User Threshold Req/2 mins Set the No of requests allowed in 2 minutes per User

API Threshold Req/2 mins Set the No of API requests allowed in 2 minutes

Traffic Access Settings

Customer can choose to enable Advance DDOS based on their need from Portal. Please do it with caution and do it at off-hours to monitor the behaviour of your site when cookies are enabled. Please contact [Support](#) for any help.

When to enable Advance DDOS?

We recommend Advance DDOS to be enabled for all sites. With advance DDOS enabled tracking comes down to very granular level i.e.) Per browser session and it will be hard for attackers/bots to replicate a genuine user. That said, please be aware that enabling this would mean, AppTrana will be injecting a cookie for any user trying to access your site.



If your site is under attack or you are seeing any abnormal number of requests to backend server which you think can be malicious, then we recommend you to enable Advance DDOS which will eventually track and automatically block malicious bots and user access.

Please reach out to [Indusface Support](#) if you have any questions