OMAN DATAPARK

Web Application Firewall(WAF)

A Web Application Firewall That Guards Your Critical Applications

1. Introduction

The Web Application Firewall referred to as "WAF", it protects your website against OWASP top 10 threats, application vulnerabilities, & zero-day attacks.

Leading Layer 7 DDoS defenses, detection & mitigation techniques, virtual patching, & granular attack visibility thwart even the most sophisticated threats before they reach your servers. The WAF also enables compliance with key regulatory standards like HIPAA & PCI-DSS.

With the WAF, you will gain the flexibility your website requires to deploy the Web Application Firewall (WAF) services & protect it wherever it resides, whether within a virtual software, a defined data center (SDDC), A managed cloud service environment, public cloud, or traditional data center.

The WAF will protect against web application attacks such as:

1. Cookies/hidden fields manipulation.
2. SQL injection attacks.
3. Malicious exploitations of the application memory buffer.
4. Unauthorized user access to authenticated accounts using cross-site request forgery (CSRF).
5. Unauthorized changes to server content.
6. Attempts aimed at causing the web application to be unavailable or to respond slowly.
7. Layer 7 denial-of-service, brute force, and web scraping attacks.
8. Zero-day threats.
9. Access from unauthorized IP addresses or geolocations.

2. Web Application Firewall Benefits

1. Securing web applications against vulnerabilities & known attack patterns, protecting sensitive data, & proactively identifying (& possibly blocking) attackers performing unauthorized activities.

2. Restrict access to a web application only from those locations identified on a whitelist or to prevent access from certain geolocations.

3. Address external traffic vulnerability issues that might not be cost effective to address at the application level.

4. Be an interim solution while an application is being developed or modified to address vulnerability issues.

5. Quickly respond to new threats. You can tune WAF to block new threats within a few hours of detection if needed.

These are just a few of the ways that WAF can be used to secure your web applications.

3. Information Gathering list

Please fill the below list in order to smoothly configure & activate the WAF on your website:

WAF Prerequisite:	**Client Feedback:**
Website URL:	
Website Server IP Address:	
Dedicated IP's for WAF (4 Private IP's):	
Website Operating System:	
Web Server (Apache Tomcat, apache HTTP, IIS, Proxy, etc.):	
Languages & Applications (ASP, ASP.NET, CGI, Front Page, Java Servlets/JSP, Lotus Domino, Macromedia Coldfusion,, Macromedia JRun, Outlook Web Access, PHP, SSI (Server Side Includes), WEbDAV, XML):	
Database Servers (IBM DB2, MSSQL Server, MySQL, Oracle, Postgre SQL, Sybase/ASE):	
Does the website have an SSL page?	
Does the website have an administrator login page? (if yes, kindly share the URL, Admin page must be tested in Learning Period to allow legitimate admin actions)	
Does the website receive/post specific file uploads from/to end users? (if yes, kindly share the file type)	
Does the website have an electronic form? (if yes, kindly share an example of a filled e-form)	

4. Activation Process

The WAF activation process will go through 2 phases: *Transparent (Learn)* mode & *Blocking (Protect) mode*.

Transparent (Learn) mode: it will learn the legitimate traffic of your website for a duration of 7 days, in order to differentiate it from suspicious requests & set policies based on what is accessing your website regularly; it will not block anything during this phase.

Blocking (Protect) mode: it will protect your website against suspicious & abnormal web requests as well as known web attacks.

Following are the WAF Activation Steps:

1. ODP will receive the full prerequisite information from the client.
2. After completing the configuration, the WAF will be activated and set in learning mode for 7 days.
3. During learning mode, the WAF will go through fine tuning to learn the valid website traffic.
4. After 7 days, the WAF will be switched to the Blocking (Protect) mode where every suspicious request will not reach the website.
5. In case of any false positives, the website will show a *support ID*, kindly send us the support ID in order to allow legitimate traffic.