eNlight WAF Datasheet

eNlight WAF is specially engineered intelligent Cloud Hosted Web Application Firewall that allows you to filter incoming and outgoing web traffic and block threats like injection, cross site scripting and other attacks of the OWASP Top10. It also allows the user to create custom rules for blocking web attacks. The illegitimate traffic gets block automatically by the eNlight WAF when anomaly threshold reaches and the custom response is sent to the attacker.

With eNlight WAF, you pay as you grow. Billing is done on your eNlight Cloud VM resource usage. Multiple websites can be added on eNlight WAF.

WAF also provides clientless VPN(WebVPN) solution for your private applications.

eNlight WAF Features

Security

Enable TLS, control user reputation, set up access control and block OWASP Top 10 attacks (XSS, SQL Injection, Malware) before they reach your web applications

High Availability

Need to increase the traffic handling capacity? Add nodes to the cluster: WAF runs natively as active/active and supports the CARP virtual addresses.

Load Distribution

With HA-Proxy, WAF distributes incoming traffic to all nodes in the cluster. WAF can then dispatch the traffic to a farm of Web servers.

Content Rewriting

WAF works in reverse-proxy. You can rewrite links, headers, content, compress pages.

Anomaly Detection

WAF integrates anomaly detection algorithms allowing the administrator to identify risky behaviors and create effective filtering policies. No need to invest in a SIEM to benefit log analysis, alerting or anomaly detection in real time.

WebVPN

WAF provides client less VPN solution to access privately hosted application over internet with authentication and high security.

eNlight WAF Architecture

- eNlight WAF scans website traffic and automatically filters out legitimate traffic based on the rule sets.
- eNlight WAF sends a custom response code and message when an attack incident is detected. It records all attack incidents.
- DNS redirection is required for web applications.

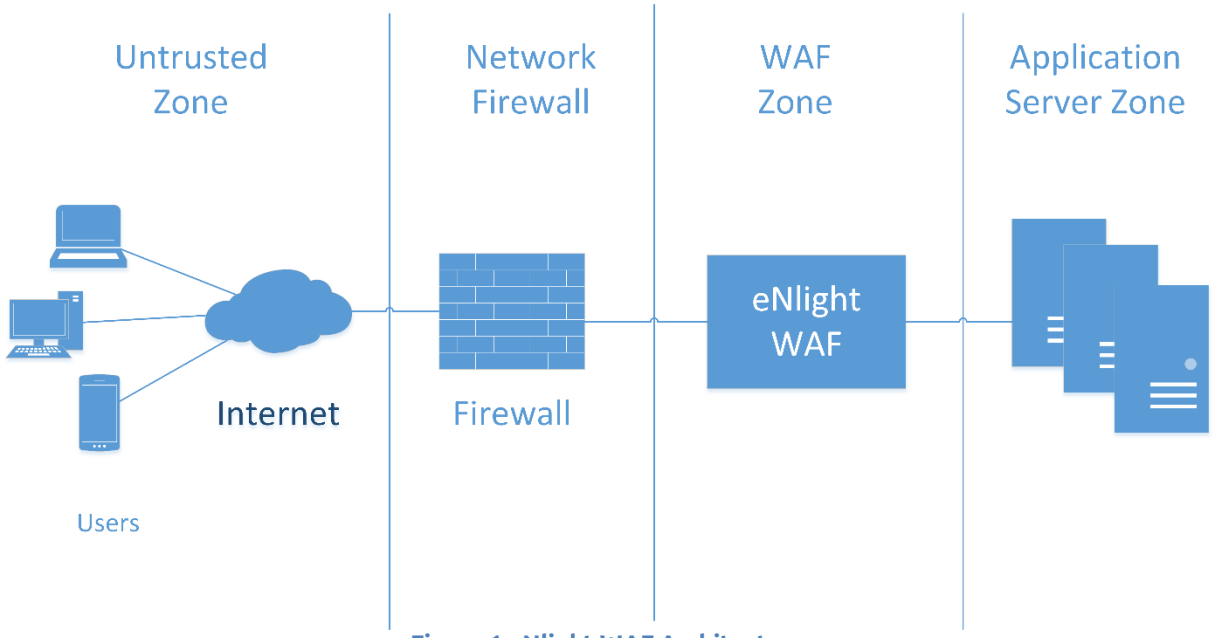

Figure 1 eNlight WAF Architecture

eNlight WAF Technical Specs

- Web Load Balancer

WAF can spread the load over multiple web servers and maintain application sessions.

- Load-balancing IPv4/IPv6 network

Inbound traffic is distributed to all nodes in the cluster IPv4/IPv6 virtual addresses

If one node fails, the others take over IPv4/IPv6 network firewall. Malicious IPs are blocked before they reach applications.

- Source IP Reputation Analysis

WAF geo-localizes source IPs and analyzes their reputation It is possible to make filtering policies on these criteria. The blocking is done before processing the HTTP request.

- Learning Mode

WAF records all suspicious requests without blocking the user. Administrator manages false positives without hindering user activity. When there is no more blocking identified, the learning mode is disabled and WAF goes into blocking mode.

- Machine Learning

In addition to rule-based filtering and reputation of the sources, WAF proposes an approach based on mathematical algorithms:

1. Learning and modeling of typical traffic

2. Detection of "abnormal" requests

- Log Analyzer

The logs are searchable from the administration interface. Quick and intuitive interface, possibility to save your search filters. Logs available: Firewall, WAF, access to applications, internal logs (API, diagnostic system etc.).

- Supports multiple websites security

Supposing an organization has more than one website and wants to handle all the websites by eNlight WAF, that's possible with a single dashboard multiple websites can be handled.

- Virtual Patching

Upload a vulnerability scanner report, WAF generates the rules to correct the identified vulnerabilities.

- Scoring Policy

WAF makes the decision to block when the risk score exceeds the threshold tolerated. The administrator decides score threshold policy.

- OWASP Top 10 Protection

Qualified and ready-to-use rules are integrated by default. Protection against OWASP Top 10 vulnerabilities. Automatic import, versioning rule sets, graphical interface to edit the rules, assistant for writing rules.

eNlight WAF Specifications

Minimum Required Sizing For WAF		
Specifications	**CPU**	**RAM (MB)**
Minimum WAF VM Sizing	1	512
Minimum Webserver Size	1	512

No. of Request getting accommodate for Minimum Configuration	
Request Per Second	232.01
Request Per Min	13920.6
Request Per Hour	835236
Request Per Day	20045664

Configuration wise User Accommodation		
CPU (vCPU)	**RAM (GB)**	**Users**
2	2	100
4	4	500
8	8	1000