Comprehensive Protection from Web Hacking

DDoS + WAF Protection. No Other Compares.

Owing to the growing cyber-threat, the need for a cloud-based web application firewall (WAF) has never been more necessary. A cloud-based WAF is deployed between the web servers and the Internet, inspecting and filtering incoming and outgoing traffic. Once configured with known malicious HTTP-based attacks, the WAF monitors and blocks such content and requests that do not match the designated rule-set.

This defense mechanism is effective in protecting your organisational applications against a wide range of unwanted threats and malicious attacks, such as SQL injections, cross-site scripting and other threats. Without WAF protection, your web server may be compromised and your confidential data may be stolen by hackers.

Unlike just a few years ago when WAFs were only available as a form of hardware appliance, our service plans include a cloud-based WAF module offering you a higher level of security previously affordable to larger organisations. Our WAF is integrated into our comprehensive cybersecurity solution. Together the solution protect public-facing websites from large-scale layer 3/4 DDoS attacks and more complex layer 7 hacking and DDoS attacks.

Better still, we have a 24x7 team of security experts at our Security Operations Centre (SOC) constantly monitoring and tuning it to protect you from evolving threats. And unlike appliance-based solution, we centrally manage our WAF platform, therefore threat detection is shared among other clients, resulting in improved detection rates as well as lower false positives.

How does it work?

WAF stops attacks at the network edge, protecting your websites from common threats and specialized attacks before they reach your web servers.

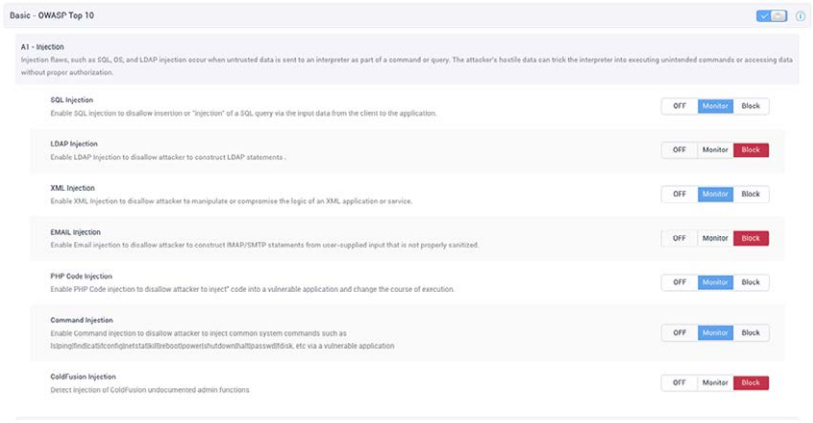
It examines within the data payload, beyond simply the IP or TCP headers; performs Deep Packet Inspection (DPI); and detects and responds to signatures for known application vulnerabilities. However, it does not require modifications to existing application code.

Features

Protection against OWASP Top 10 common vulnerabilities

The default rule set developed and maintained by service provider, ensuring that you are protected against the OWASP Top 10 common vulnerabilities:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Unvalidated Redirects and Forwards



The rule set also comprises our own rule sets and custom rules defined by the client. Our WAF engineers can work with the customer to develop and refine site-/application-specific rules.

Features

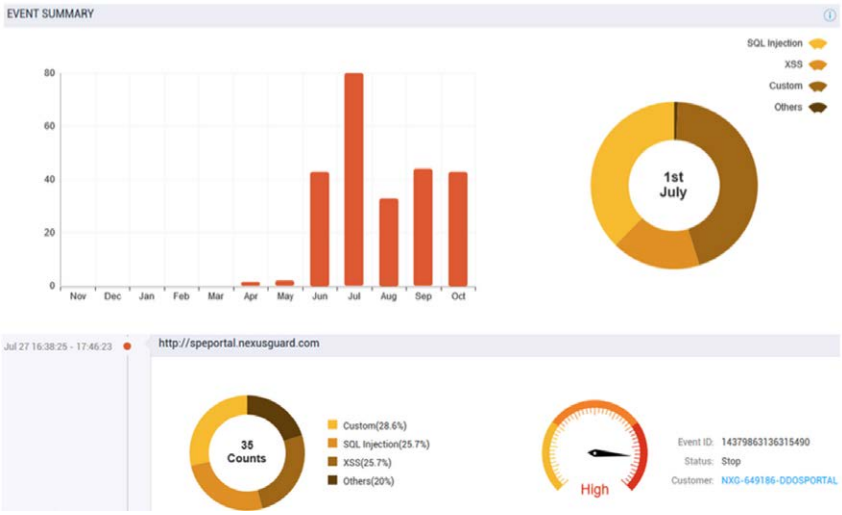
- Protection against OWASP Top 10 common vulnerabilities
- Custom Rules
- Botnet Attack Protection
- Automatic Virtual Patches
- Real-time Reporting and Robust Logging
- Easy installation, fast deployment
- Dedicated research team
- Ongoing fine-tuning of security rules
- 24x7x365 SOCs

Custom Rules

Custom rules can be used to protect your website from new attacks or tailor make security rules for your websites based on HTTP request headers such as URL, Query String, Cookie, and etc. Working in tandem with default rules, custom rules will help to tighten security policies and reduce false-positives.

Botnet Attack Protection

Our WAF is integrated into our comprehensive cybersecurity solution. Together the solution protect public-facing websites from large-scale layer 3/4 DDoS attacks and more complex layer 7 hacking and DDoS attacks that attempt to exhaust resources of web applications and servers.



Features

- Protection against OWASP Top 10 common vulnerabilities
- Custom Rules
- Botnet Attack Protection
- Automatic Virtual Patches
- Real-time Reporting and Robust Logging
- Easy installation, fast deployment
- Dedicated research team
- Ongoing fine-tuning of security rules
- 24x7x365 SOCs

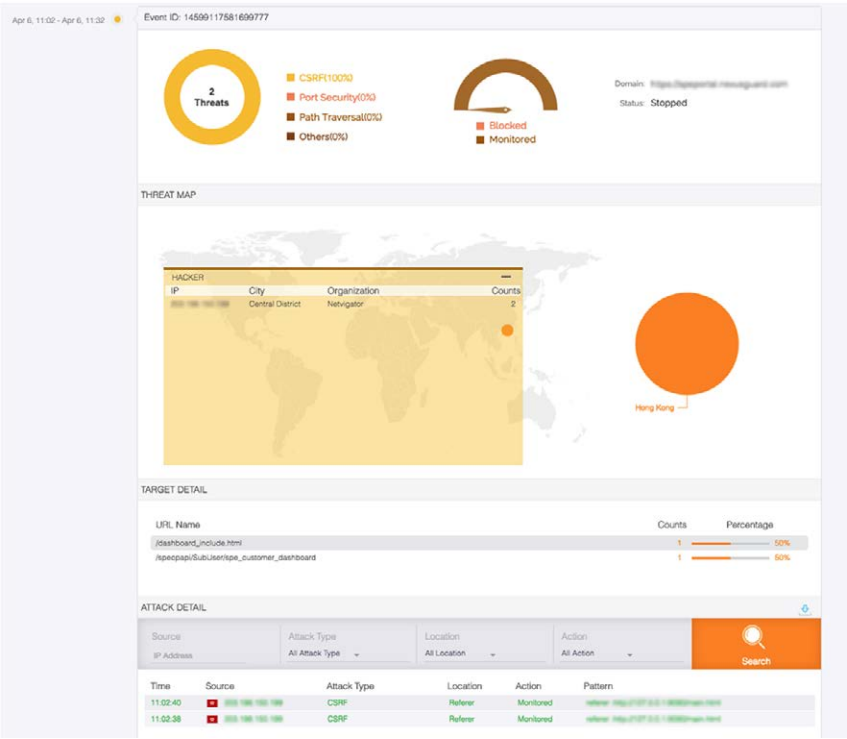
Automatic Virtual Patches

Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts. Our WAF can automatically blocks this type of vulnerability exploit attempts to your web application until either the vendor provides a permanent solution or in-house developer fixes it.

Real-time Reporting and Robust Logging

Our visually-appealing, intuitive Customer Portal features comprehensive dashboard, charts and tables, showing all ongoing and historic WAF events.

- Visualized event reports based on attack types, UID/source IPs, target websites, etc.
- WAF report analytics includes attack source, target URL, attack type and time/duration
- Real-time traffic log/packet analyzer for on-the-fly analysis; real-time global traffic map
- Free WAF event log downloads (any time)



Features

- Protection against OWASP Top 10 common vulnerabilities
- Custom Rules
- Botnet Attack Protection
- Automatic Virtual Patches
- Real-time Reporting and Robust Logging
- Easy installation, fast deployment
- Dedicated research team
- Ongoing fine-tuning of security rules
- 24x7x365 SOCs

Easy installation, fast deployment

Our cloud-based WAF is integrated into our Cybersecurity Platform as one of the security layers to deliver comprehensive protection solution. While we will do the necessary tests and define custom rule set tailored to your web applications before implementation, nothing has to be setup or configured on your side. Once testing is done, protection can be activated in just minutes with no impact on your existing infrastructure.

Dedicated research team

Behind our WAF development and operation teams it is a research team dedicated to analysis of threat intelligence collected from external and internal sources as we pursue meticulous protection against zero-day attacks and persistent threats.

Ongoing fine-tuning of security rules

Our WAF engineers constantly review and fine tune security rules to a minimum false positive rate.

24x7x365 SOCs

We have 24x7x365 SOCs staffed with DDoS and WAF experts to monitor and respond to potential threats and attacks in the shortest time possible.

Benefits

Stop DDoS and hacking attacks before reaching web server

- At the IP/TCP level (layers 3 & 4)
- At the application level (layers 7)

Faulty code will be protected from exploitation on

- Web application vulnerabilities
- Well-known web application components' vulnerabilities, such as wordpress and struts

Bandwidth cost efficiency

- We are very focused on attack mitigation, rather than absorption,
- Ensuring that bandwidth is consumed only by clean traffic and blocking malicious/attack traffic from costing you extra money in bandwidth charges

PCI DSS compliance

- Integrating our cloud-based WAF ensures compliance with PCI DSS (requirement 6.6)
- Cost-effective solution for achieving/maintaining PCI DSS compliance
- Prevent sensitive data leakage, e.g. credit card data, customer information, customer login/password, etc.
- Hedge risks of commercial costs (i.e. legal costs, compensation, etc.) arising from failures in PCI DSS compliance audits.

Maintain search engine ranking and avoid blacklisting

- Nexusguard has patented search engine crawler identification technology that accurately segregates legitimate crawlers from spoofed or illicit ones
- Free from malware, so the site won't be blacklisted by search engines

Low total cost of ownership (TCO)

As a total cloud solution, our WAF requires no hardware, software, operational and maintenance costs, nor does it need any rack space or electricity costs. No in-house WAF engineers are needed on the client side as well.

Data Sheet

NEXUSGUARD

Founded in 2008, Nexusguard is the global leader in fighting malicious internet attacks. Nexusguard protects clients against a multitude of threats, including distributed denial of service (DDoS) attacks, to ensure uninterrupted internet service. Nexusguard provides comprehensive, highly customized solutions for customers of all sizes, across a range of industries, and also enables turnkey anti-DDoS solutions for service providers. Nexusguard delivers on its promise to maximize peace of mind by minimizing threats. Headquartered in San Francisco, Nexusguard's network of security experts extends globally.

Twitter twitter.com/nexusguard
Facebook facebook.com/NXG.PR
LinkedIn linkedin.com/company/nexusguard

nexusguard.com
contact@nexusguard.com

20160413-EN-A4