Intelligent Web Application Firewall (iWAF)

Point-and-Click Simplicity for Web Application Security

CHALLENGES

- Low performance and massive variability result in scaling and capacity planning challenges
- Increasing complex process for writing security policies and rules
- Lack of visibility into how policies impact traffic flows

SOLUTION — AVI IWAF

- Instant autoscaling to handle security challenges and easy rule generation to customize response
- Real-time visibility and insights into application performance and end-user experience
- GDPR, HIPAA, and PCI compliance with config audit trail across a distributed software fabric

BENEFITS

- Elasticity with on-demand autoscaling architecture and per-app deployment / protection
- Point-and-click simplicity for policies with central control management
- Granular security insights on traffic flows and rule matches to create precise and custom policies

WEB APPLICATIONS ARE UNDER-SECURED BY TODAY'S WAFS

Web application firewalls (WAFs) are intended to protect businesses from web app attacks and proactively prevent threats. Yet, despite the potential security benefits, organizations tend to shy away from implementing WAF solutions for three key reasons:

- **Slow to scale.** Traditional WAFs are inelastic and unable to provide the scalability required for increasing volumes of encrypted traffic and variable loads. Hardware appliance-based WAFs need significant overprovisioning.
- **Complex rules**. Most WAFs today are very complicated, presenting a wall-of-knobs to administrators in order to configure security policies. Tuning rules is even more challenging, not to mention customizing for each application.
- **No visibility or intelligence**. Most WAFs today are a "black box." Once rule sets are defined, it is difficult to update, monitor and impossible to react in real time to changes or new security threats.

OPERATIONAL INTELLIGENCE THROUGH MACHINE LEARNING

VMware NSX® Advanced Load Balancer™ (by Avi Networks) leverages software-defined architecture and its strategic location on the network to gain real-time application insights. The built-in iWAF solution provides application security and networking teams with an elastic and analytics-driven solution that scales and simplifies policy customization and administration through central management. See Figure 1 for the security stack.

NSX Advanced Load Balancer
Comprehensive Security Stack

Figure 1: NSX Advanced Load Balancer Security Overview

Avi's iWAF gives administrators an important point of security enforcement and intelligence. iWAF protects web applications from common vulnerabilities as identified by Open Web Application Security Project (OWASP), such as SQL Injection (SQLi) and Cross-site Scripting (XSS), while providing the ability to customize the rule set for each application. iWAF analyzes the security rules that match a particular transaction and provides that insight in real-time as applications and attack patterns are learned. This application intelligence, paired with intuitive one-click rule customization, allows iWAF to sharply reduce false-positives.

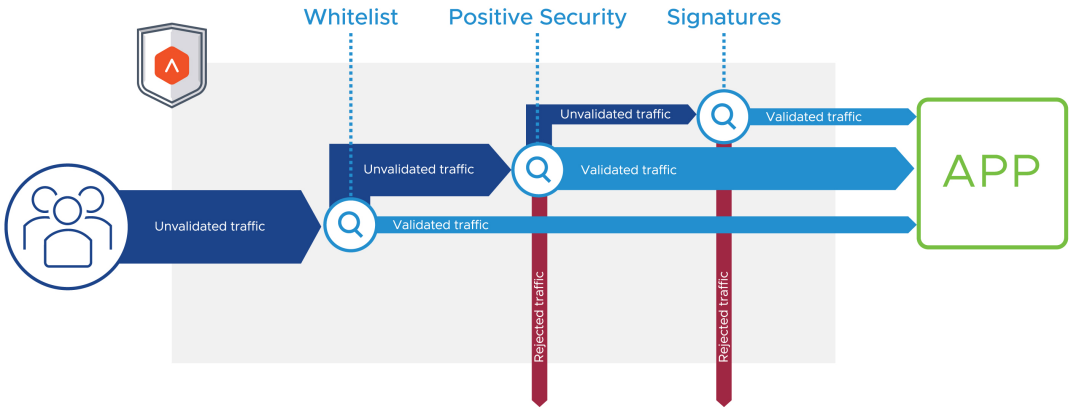

Figure 2: Avi iWAF Security Pipeline Optimization

FEATURES AT-A-GLANCE

Core Security

- **OWASP Top 10 attack protection** including HTTP validation, injection, data leakage protection, automated attack blocking and application specific security.
- **Guided false-positive mitigation** with customizable paranoia levels that control the strictness of the policy based on the logs and analytics.
- **Rate-limiting per app** to limit L3/L4 and L7 traffic based on parameters such as Client IP, URL and Path.
- **Point-and-click policy** with central control and ease of use by enabling users to create custom policies quickly and efficiently.
- **RBAC support** to control write access to WAF profiles and policies; read access to applications, pools and clouds.

Threat Detection

- **Whitelisting** rules that allow bypassing WAF for certain request properties e.g to whitelist the DAST scanner IPs from WAF inspection, to exclude internal IP addresses from WAF inspection or to bypass WAF for all POST requests.
- **Positive security** for allowed application behavior in order to block anomalies. Positive model engine is called before the signature engine, reducing false positives and time to reach a decision about the validity of the request.
- **Signatures protection** against known threats through a blacklist approach by analyzing every part of the incoming and outgoing requests against SQLi, XSS and other threats based on Core Rule Set (CRS).

Application Protection

- **Learning mode** for application behavior and structure helps profile applications, inform decisions and automatically create positive security rules.
- **Per-app deployment** for precision protection of specific applications with different security policy levels while ensuring application performance.
- **On-demand autoscaling** to elastically scale the number of WAF instances and application servers to handle unpredictable traffic without impacting performance.
- **Application analytics** for WAF events based on historical trend information and real-time visibility into ongoing operations, application behavior analysis, and attack patterns.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.