AVI Networks®

SOLUTION BRIEF

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 scaling in response to security challenges
- GDPR, HIPAA, and PCI compliance with a scalable and distributed software fabric
- Real-time visibility into application performance and end-user experience

BENEFITS

- Elasticity based on automatic scale-out scale-out architecture
- Point-and-click simplicity for policies with central control management
- Granular security insights on traffic flows and rule matches to create precise policies

Intelligent Web Application Firewall (iWAF)

Point-and-Click Simplicity for Web-Scale Security

TRADITIONAL SOLUTIONS OUTPACED BY SECURITY THREATS

Web application firewalls (WAFs) can provide businesses with the protection needed to limit web app attacks. Yet, despite the security benefits of WAFs, organizations tend to shy away from implementing appliance-based WAF solutions for three key reasons:

- **Slow to scale.** Traditional WAFs are inelastic and can't provide the scalability required for increasing, variable loads, at least not without significantly overprovisioning.
- **Complex rule writing.** Developing simple rules following Open Web Application Security Project (OWASP) best practices is time consuming, and tuning rules is even more challenging.
- **No visibility or intelligence.** Most WAFs are a "black box." Once rule sets are defined, it is difficult to monitor and impossible to react in real-time to changes or new security threats.

OPERATIONAL INTELLIGENCE THROUGH MACHINE LEARNING

Avi iWAF leverages software-defined architecture and its strategic location on the network to gain real-time application insights. iWAF provides application security teams with an elastic and analytics-driven solution that scales and simplifies policy customization and administration through central management. See Figure 1.

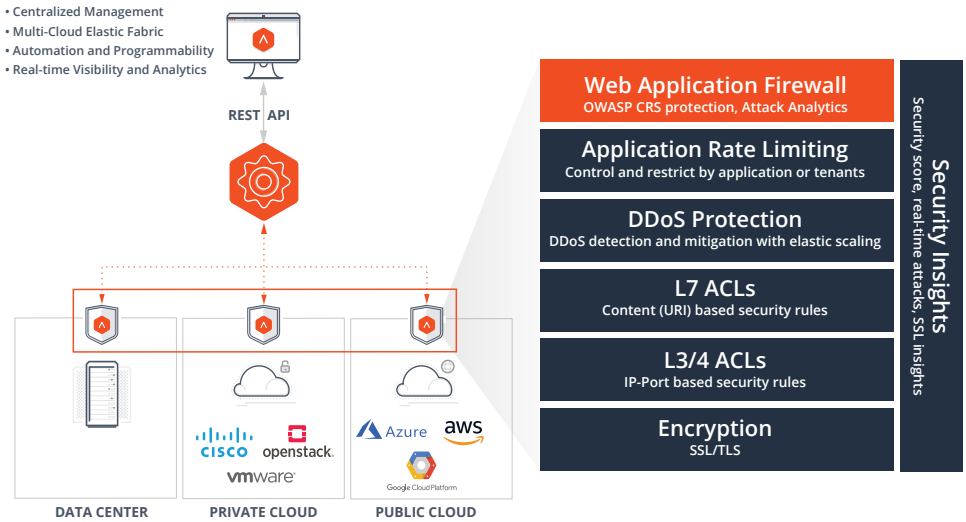

Figure 1: Avi Security Overview

Avi's iWAF is an important source 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 and Cross-site Scripting, while providing the ability to customize the rule set for each application. iWAF analyzes the security rules that match a particular transaction, providing this insight in real-time as applications and attack patterns evolve. This application intelligence, paired with intuitive one-click rule customization, allows iWAF to sharply reduce false-positives. See Figure 2.

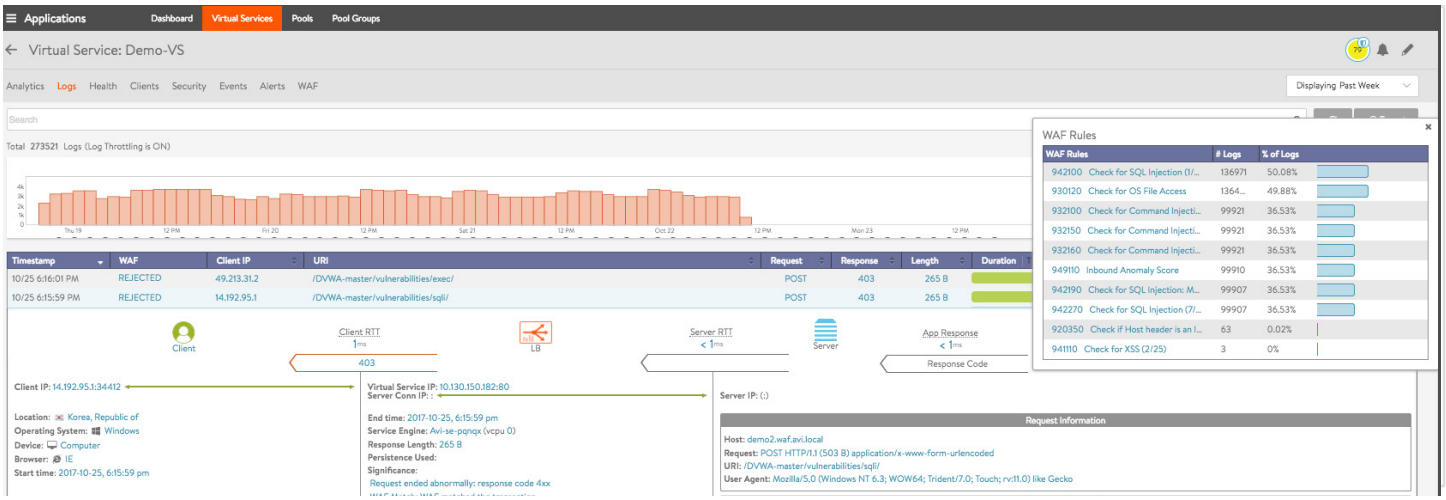

Figure 2: Security Insights and WAF Rules

AVI IWAF: USE CASES

Integrity Check

- Input protection (SQL Injection, Cross-site Scripting (XSS), local/ remote file inclusion, remote code execution, PHP code injection, path traversal, session fixation)
- HTTP validation (limit HTTP allow method, encoding bypass detection, HTTP response splitting, HTTP parameter pollution)

Threat Detection

- Protection against 0-day attacks (Shellshock, httpoxy)
- Automated attack blocking (scanner detection, brute force attacks (rate limiting))
- IP protection (GeoIP blocking)

Application Protection

- Data leakage protection (error message suppression, leakage of personally identifiable information such as credit card or SSN numbers)
- Application specific security (Drupal, Wordpress)

AVI IWAF: BENEFITS

Central, Scalable Policy Management

- Central management of all distributed iWAF in-stances
- Point-and-click policy configurations, customizable for each application

Analytics-Driven, Accurate Security Policies

- Elimination of false positives with security insights
- Visual policy checks prior to enforcement

High-Performance Web Application Security

- Automated configurations with REST API
- Per-app deployments and elastic scaling across data centers and clouds