Web Application and API Protection – Ingress Security

Automated and Elastic Application Security

Comprehensive App Security

- Robust API protection
- Context-aware web application firewall
- Intelligent bot management
- Powerful SSL offload
- Advanced DDoS detection/mitigation
- Enhanced authentication

> "We had a large volume of users and quickly ran into performance issues with our appliance-based load balancer and WAF solutions. The lack of elasticity and poor performance was impacting our ability to deliver a great experience for customers of our internet gaming platform."
>
> JORIS VUFFRAY
> Head of Network and
> System Management
> Swisslos

Application security is complicated and even more so in this multi-cloud, multi-platform IT environment. Businesses are challenged with building a robust and secure IT architecture that can deliver their applications reliably and securely. 94% of enterprises are moving to the multi-cloud. At the same time, 88% are adopting microservices architectures[1].

These two trends are driving much of the transformation and innovation today, mandating a new approach to application delivery and security. IT needs to be multi-faceted and incorporated at every point in the design where feasible. But it is the ingress, or entry point to the application network where applications are exposed to known and unknown threats.

First Line of App Defense

VMware is addressing ingress app security with VMware NSX Advanced Load Balancer (Avi). Avi delivers an integrated application delivery and security platform that is simple to use, robust, and scalable platform with advanced features to protect applications and their APIs (see Figure 1).

Avi's web app and API protection (WAAP) offers key protection against different security threats entering the application hosting environment. These include API protection, Web Application Firewall (WAF), SSL Offload, DDoS detection and mitigation, bot detection and management, and authentication.

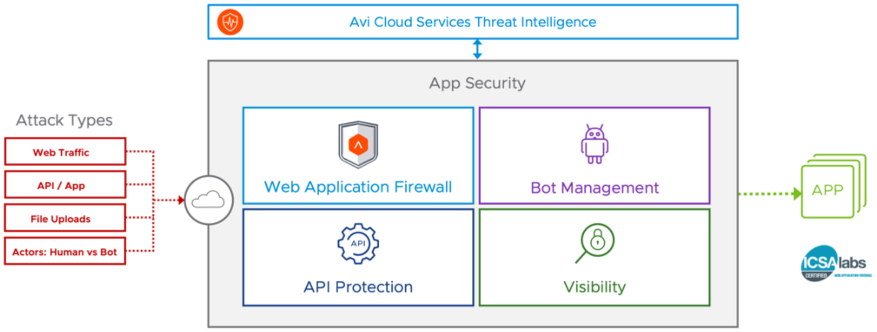

Figure 1: Inline integrated ingress protection for all attack types

[1] Source: Pulse Survey, February 2022 [add link, can be found on resources]

Simple and Integrated Ingress Protection

Most of the threats entering the application environment are external threats coming from outside. The ingress point is the critical security point to detect and block the majority of threats while complimenting the other tiered security solutions including such as next-gen firewalls, end point detection and protection (EDP), and anti-virus/malware detection.

The solution can detect and block multiple types of security threats in an easy to consume manner. This means it supports a broad spectrum of capabilities and can be managed through a central unified platform. Security policies are easy to configure and fine tune. The solution is robust and scalable without any performance impact and can react to security attacks quickly.

Ingress security requires a comprehensive solution that can detect and manage many different attack vectors. A simple, but comprehensive view of the traffic and security alerts is needed to ease the operational burden of maintaining a secure application delivery infrastructure. Automation and analytics reduce the manual labor required to manage the influx of information.

Optimally, the solution should offer:

Simplicity: A comprehensive, but simple to deploy and manage ingress solution is critical. Current application architectures are complex and it is impossible to effectively manage them manually. A security architecture that can separate the control plane from the data plane delivers a centralized point of control for configuring and monitoring the complicated security policies. Detailed visibility and intelligent analytics improve the operational management of the solution.

Context-Aware: Context-aware security solutions are necessary for today's applications. It is important to how and why applications are using the data. This is essential to meet compliance standards such as PCI-DSS, HIPAA, and GDPR. Context-aware solutions understand the application behavior and can provide tailored security policies without overburdening the security operations team. Real-time updates to the security policies from a trusted service like Avi Pulse can protect against present and future threats, known and unknown.

Elasticity: Elasticity is essential in today's dynamic application delivery environments. Applications are being deployed across multiple clouds. Microservices mean that application instances are being created and removed regularly to match client demand. The ingress security solution must be able to scale up and down along with the application in real-time.

Web App Protection and Security for Today and Tomorrow

Avi's technology is designed for the modern application architecture. Multi-cloud and containers mean that technologies must shift from a legacy appliance-based architecture to a more flexible and dynamic model.

Avi delivers a full featured ingress security solution to meet today's application environments whether in legacy datacenters, multi-cloud, or in containerized microservices environments. The automation and analytics enhance the security operations and streamlines the DevOps process.

Learn more at https://avinetworks.com/web-application-security/