

SECURITY INSIGHTS WITH iWAF

For security, Avi features an Intelligent Web Application Firewall (iWAF) with distributed web application security fabric to enforce security through closed-loop analytics and application learning mode that covers OWASP CRS protection, support for compliance regulations such as PCI DSS, HIPAA, and GDPR, and signature-based detection. iWAF provides an optimized security pipeline with positive security model to maximize the efficiency for resource intensive operations. Avi Pulse cloud services provide live feeds of new threat updates including IP reputation, bot detection, signatures and more, and automatically minimize false positives with advanced security analytics, detection, and enforcement modes. With real-time app security insights and analytics provide actionable insights on performance, end-users and security events in a single dashboard (Avi App Insights) with end-to-end visibility. See Figure 2.

KEY FEATURES

- Point-and-click simplicity for security policies with central control
- Elastic scale with high performing, load based automatic scale-out architecture
- Granular security insights on traffic flows and rule matches for precise policies
- Automated threat updates through Avi Pulse Services
- Real-time app security insights and analytics
- Protects applications from DDoS attacks and OWASP Top 10 threats

FIGURE 2: iWAF Security Insights for Web Applications

KUBERNETES INGRESS SERVICES

Modern application architectures based on microservices have made appliance-based load balancing solutions obsolete. Containerized applications deployed in Kubernetes clusters need a scalable and enterprise-class solution for load balancing, global and local traffic management, service discovery, monitoring/analytics, and security. However, not in a disparate way with siloed DIY products to be stitched all by the platform teams. Enterprises adopting Kubernetes need a cloud-native approach for traffic management and application networking services. For modern container-based applications, NSX Advanced Load Balancer offers a consolidated set of container services including cloud-native, scalable, enterprise-class container ingress traffic management, dynamic service discovery, and security. See Figure 3

KEY FEATURES

Traffic Management & Service Discovery

- Local and global load balancing
- DNS / IPAM / Circuit Breaking
- Health Monitoring
- TLS termination, Cert management / automation
- CI/CD and Blue-Green / Canary deployments

Security & Observability

- WAF
- Authentication
- Acceptlist / Denylist
- Rate Limiting
- DOS detection / mitigation
- Application and infra performance metrics
- Transaction tracing & fine-grained logging

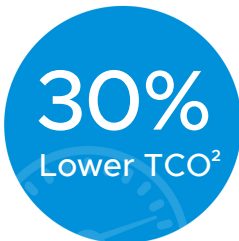
FIGURE 3: Avi Kubernetes Ingress Services



AGILITY FROM AUTOMATED PROVISIONING AND SELF-SERVICE

Automated virtual service provisioning with per-app load balancing services

- Virtual IP (VIP) provisioning in seconds
- Full automation with REST APIs to support faster application rollout in Blue/Green and Canary deployments and enable DevOps teams with self-service portals
- Simplified operations with centralized policies
- Full lifecycle management through application delivery automation
- No manual per appliance configurations



LOWER COST WITH SIMPLIFIED OPERATIONS

Elastic load balancing and just-right-size capacity without overprovisioning

- No overprovisioned capacity and continuous refresh, upgrades and maintenance of individual hardware appliances
- Flexible, subscription- based licensing model that eliminates static capacity
- Reduced OpEx through simplified operations of central management
- No custom active-standby hardware needed with software-defined load balancing on high-performance Intel x86 servers
- Consistent application services across multi-cloud environments without reconfiguration



RAPID RESOLUTION IN SECONDS

Google-search like visibility into network transactions to troubleshoot quickly

- Application health score for a quick snapshot of network posture
- End-to-end round-trip times with latencies between each network hop
- Real-time logging, recording and replaying traffic events
- Granular insights into performance, security, and end user experience
- Point-and-click application troubleshooting – no black box



ELASTIC AUTOSCALING AND HIGH PERFORMANCE

On-demand scale up or down using analytics-driven automation based on real-time traffic

- Self-service provisioning for continuous application delivery
- CI/CD support On-demand load balancing and application autoscaling
- Service Engine failure auto recovery
- Automatically programs network, cloud, and app environments
 - Full support for multi cloud - On-Premises mixed with Azure, AWS, Google Cloud Platform

1. *The Business Value of Avi Vantage: A Study of Enterprises Using Next-Generation Application Delivery*

2. *VMware Data Integrated Customer Engagement (DICE) Tool*

3. *Load Balancing Benchmark Report by Principled Technologies*

SUPPORTED PLATFORMS		SYSTEM PERFORMANCE AND SCALE	
VMware	vCenter, VMware NSX, VMware Cloud on AWS	Max System Throughput	10 Tbps
OpenStack	Queens, Rocky, Stein, RH OSP, Keystone v3	Max Connections	100 million per second
Bare Metal	RHEL, CentOS, Ubuntu, Oracle Enterprise Linux, Cisco CSP (NFV appliance)	Max Concurrent Connections	10 billion
Containers	Kubernetes, OpenShift, Amazon EKS, AKS, GKE	Max HTTP Requests	200 million per second
Public Cloud	Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), IBM Cloud, Oracle Cloud	Max SSL TPS (2k RSA)	10 million
SDN	Cisco ACI/APIC, VMware NSX, Nuage VSP, Juniper Contrail	Max SSL TPS (SEC256r1 ECC)	30 million
IPAM / DNS	Avi DNS, Azure DNS, Azure DNS Private Zones, AWS Route 53, Infoblox, Custom DNS integration	Max tenants (shared data plane)	Unlimited
Automation	Ansible, Terraform, Swagger, Python SDK, Go SDK, vRealize Orchestrator (vRO), Native REST API	Max tenants (isolated data plane)	200
Monitoring	Splunk, Cisco Tetration, Cisco AppDynamics, Graphite, Datadog, Logstash, Elasticsearch, InfluxDB, Syslog, Prometheus, Zabbix	Max Avi Service Engines	200

FEATURE	DESCRIPTION
Enterprise-class load balancing	TLS 1.3 support, SSL termination, default gateway, GSLB, DNS, wildcard VIP and other L4-L7 services
Multi-cloud load balancing	Intelligent traffic routing across multiple sites and across private or public clouds, global server load balancing supported with Canary upgrades of leader and follower sites
Application performance monitoring	Monitor performance and record and replay network events with granular logging
Predictive autoscaling	Application and load balancer scaling based on real-time traffic patterns
Cloud connectors	VMware, SDN controllers, OpenStack, AWS, GCP, Azure, Linux Server Cloud, OpenShift/Kubernetes, VMware Cloud on AWS (customer-managed)
Distributed application security fabric	Granular app insights from distributed service proxies to secure web apps in real time
Application security	Positive security model and learning mode for web application firewall (WAF)
SSO / Client Authentication	SAML 2.0 authentication and authorization for back-end HTTP applications
Automation and programmability	REST API based solution for accelerated application delivery, extending automation from networking to developers with self-service portal enabled
Application analytics	Real-time telemetry from a distributed load balancing fabric that delivers millions of data points in real time
Centralized management and upgrade	Policy-based management and ability to selectively upgrade data plane with Flexible Upgrade
Networking protocols support	BGP, RHI and ECMP, BFD, IPv6, VLAN & trunking, VRF awareness
Consolidated container services	Kubernetes Services including ingress, WAF, GSLB, DNS/IPAM on a scalable platform with support for multi-cluster, multi-site and multi-AZ container clusters

