radware

DefensePro VA for the Public Cloud
Data Sheet

Protecting the Public Cloud with DefensePro VA

As organizations migrate their workloads to public clouds, cybercriminals continue to develop attack tools and strategies to cause harm and impact virtual private cloud (VPC) performance. Cloud computing vendors offer limited Layer 3/Layer 4 DDoS protection, and minimal Layer 7 WAF defenses, leading to VPC outages and excessive usage penalties.

Radware DefensePro VA for the Public Cloud offers the most advanced DDoS protection for Amazon Web Services and Microsoft Azure. Based on Radware's industry-leading DDoS protection appliance, DefensePro VA for the Public Cloud protects organizations using behavioral mitigation technology against sophisticated Layer 3 – Layer 7 floods, encrypted attacks, in-session and east-west attacks.

Radware's DefensePro VA for the Public Cloud safeguards workloads from cyberthreats with a low false positive rate to provide a flawless user experience. It helps organizations ensure the availability and performance of their VPC.

AUTOMATED ZERO-DAY ATTACK DEFENSE

Behavioral-based detection and mitigation, including real-time signature creation, to defend against unknown, zero-day attacks without impacting user experience.

ADVANCED ATTACK PROTECTION

Detection and mitigation of today's most advanced attacks, including Layer 7, burst attacks, DNS amplification attacks, IoT-botnet floods and other DDoS attacks.

KEYLESS SSL/TLS FLOOD MITIGATION

High capacity keyless protection from SSL/TLS-based DDoS attacks without adding latency to customer communications while preserving user privacy.

ACCURATE NETWORK FLOOD MITIGATION

Machine learning algorithms detect and block L3/4 volumetric floods, including accurate protection of UDP-based applications and services.

How Radware Keeps your Workloads Secure from DDoS Attacks

IPS Module and Subscriptions

A dedicated module that blocks threats and prevents intruders from entering public workloads, with preemptive intel based on Radware's ERT signatures and feeds.

Dedicated Per-Application Policy

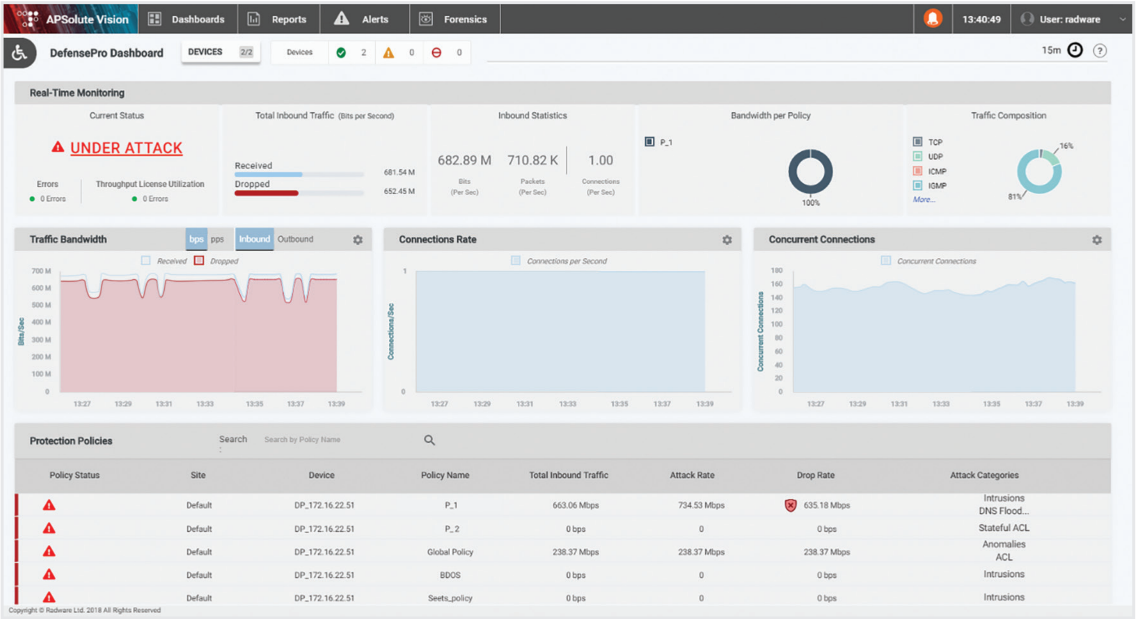
DefensePro VA allows organizations to use customized and precise DDoS protections tailored to applications needs with the ability to migrate their existing on-premise policies.

Cross Platform Management

A single technology stack across various public cloud workloads and legacy data centers with a single-pane-of-glass.

Widest Attack Coverage With The Most Advanced Technology

1. Comprehensive Layer 3 – 7 behavioral protection against known and zero-day DoS/DDoS attacks that misuse EC2, S3 and other VPC resources with no impact on legitimate traffic.
2. Burst attack protection provides immediate, behavioral-based detection and mitigation from one of today's top threats with signature creation and instant enforcement for the fastest remediation.
3. In-session flood protection to protect against sophisticated floods in existing sessions for both UDP and TCP traffic. In-session protection defends against exploitation of public cloud vulnerabilities that can cause outages to hosted applications.
4. Protection at all four fronts with bi-directional visibility to defend against sophisticated east-west attacks that go under the radar, in addition to floods that saturate the VPC's egress pipe.
5. Patent-protected stateless and keyless SSL/TLS attack mitigation solution that protects the VPC from all types of encrypted attacks with a reduced-latency and high capacity protection.
6. Automation and programmability so organizations can deploy and configure DefensePro VA using either 3rd-party infrastructure -as-code native or third-party toolsets, such as AWS CloudFormation and Terraform.
7. Advanced management & analytics for DDoS protection across cloud and on-premise environments to ensure consistent and cohesive policy and cross-platform attack forensics.



Policy Status	Site	Device	Policy Name	Total Inbound Traffic	Attack Rate	Drop Rate	Attack Categories
⚠	Default	DP_172.16.22.51	P_1	663.06 Mbps	734.53 Mbps	635.18 Mbps	Intrusions DNS Flood...
⚠	Default	DP_172.16.22.51	P_2	0 bps	0	0 bps	Stateful ACL
⚠	Default	DP_172.16.22.51	Global Policy	238.37 Mbps	238.37 Mbps	238.37 Mbps	Anomalies ACL
⚠	Default	DP_172.16.22.51	BDOS	0 bps	0	0 bps	Intrusions
⚠	Default	DP_172.16.22.51	Seets_policy	0 bps	0	0 bps	Intrusions

*A centralized dashboard to display threats in real-time with the ability to drill-down to each attack for advanced visibility into attack's data and characteristics

Ongoing Threat Intelligence and Security Expert Support

Security Update Subscription - ongoing provisioning of attack signatures for known attack types based on Radware's security research team.

ERT Active Attackers Feed - automated updates to enable blocking of attack sources actively involved in DDoS attacks.

Location-Based Mitigation (GeoIP) - network traffic filtering of countries and regions based on geolocation mapping of IP subnets.

ERT Service and Device Management - Offering 24/7, direct access to security experts for support and assistance against persistent attacks as well as on-premise device management and configuration.