radware

White Paper

Breaking the Mold: Why the Legacy ADC Paradigm No Longer Fits Modern Application Needs

Table of Contents

Introduction

In the evolving tech landscape, Application Delivery Controllers (ADCs) have been crucial in ensuring application availability and basic protection. Traditionally, ADCs focused on preventing single points of failure and maintaining performance by directing traffic to the most available servers.

However, the rise of multi-cloud environments and sophisticated cyber-threats has introduced new challenges. Modern applications now demand agility across multiple sites with faster operations and comprehensive application protection, while enabling more self-service operations and relying less on ADC and security experts. Actionable SLA visibility has also become critical, especially when operating across multiple clouds and environments. Additionally, there is a strong expectation for total cost of ownership (TCO) optimization.

Many current ADC solutions, designed with the paradigms of stable on-premises data centers, often struggle with these demands. They face inefficiencies in multi-cloud operations, application protection, and access management, and rely heavily on specialized expertise. Furthermore, visibility tools for monitoring and troubleshooting are often inadequate, leading to significant long-term costs.

As we explore the needs of modern application environments and the limitations of traditional ADC paradigms, it becomes evident that a modernized approach is essential to meet today's digital challenges.

Catalyst for Change: Identifying Modern ADC Challenges & Needs

As organizations navigate the complexities of modern application environments, their needs have evolved significantly. The traditional goals of availability and performance remain crucial, but additional requirements have emerged to address the dynamic nature of today's digital landscape.

The Complexity of Adapting to a Dynamic Application Landscape

Challenges: Both the application and business landscapes are characterized by rapidly changing requirements, necessitating quick adaptation. In today's multi-cloud world, ADC agility is paramount. Organizations face the challenge of operating across diverse environments and cloud platforms, such as OpenStack, VMware, Azure, AWS, GCP, and others. This complexity demands a unified approach to simplify management and operation, allowing teams to master a single system. The need to deploy, move, scale, or ensure high availability for applications across different environments without adapting to multiple systems is critical.

Needs: Consistent functionality and performance, along with smooth transitions across all environments, are essential to meet dynamic business demands. This agility is crucial for organizations to remain responsive and competitive in a fast-paced, multi-cloud ecosystem.

Overwhelmed by Complexity: ADC Integrated Application Protection Challenges

Challenges: As the application threat landscape evolves, protecting against an increasing number of threat vectors has become more complex. ADCs, which front-end applications, are ideally positioned to provide this protection. However, the traditional approach of integrating a Web Application Firewall (WAF) module into the ADC is no longer sufficient. Modern threats require more advanced and adaptive protection measures. Additionally, there is a global shortage of cyber protection experts, making it difficult for organizations to maintain the necessary expertise in-house.

Needs: Modern ADCs must keep protection measures up to date against evolving threats. There is a critical need to reduce management overhead and dependency on experts, given the shortage of cyber protection professionals. Solutions must be scalable to handle increasing demands without requiring periodic forklift upgrades. Ensuring application availability and safeguarding data from breaches are fundamental goals that must be met to maintain robust security in a dynamic threat environment.

Stuck in the Past: The Challenge of Outdated Access Management

Challenges: Effective user access management, including Single Sign-On (SSO), is critical for modern organizations. Traditional identity verification solutions and protocols, often based on on-premise systems, are increasingly outdated and difficult to maintain. These legacy systems struggle with issues related to interoperability, obsolete technologies, and outdated protocols, making them inefficient and prone to security vulnerabilities.

Needs: Modern organizations require access management solutions that are streamlined and efficient, and that can integrate seamlessly with advanced access management services, such as those provided by Okta and Azure. These services are constantly evolving to ensure security and augment user experience, eliminating the friction associated with outdated systems.

Transitioning to Proactive SLA Management: Key Challenges and Needs

Challenges: Traditional ADCs provided very limited and often unhelpful monitoring data. When application administrators complained about network-related performance issues, infrastructure administrators had to search for problems that often didn't exist, as the root cause was frequently on the application side. This reactive approach to problem-solving was inefficient and time-consuming, preventing proactive management and timely resolution of issues.

Needs: There is a critical need for tools that empower administrators to detect SLA problems before they impact users. Additionally, there is a need for tools that expedite root cause analysis and facilitate faster problem resolution. Addressing these needs is essential to empower ADC and infrastructure administrators to take a proactive role in managing the SLA of applications and services.

ADC Services Automation: Addressing Operational Challenges

Challenges: ADC solutions have traditionally required expert, high-touch operations, introducing significant overhead and creating bottlenecks. This reliance on specialized knowledge and manual processes often leads to inefficiencies and delays in provisioning and maintaining ADC services. The complexity of managing ADCs across diverse environments further exacerbates these issues, making it difficult for organizations to achieve the desired level of agility and responsiveness.

Needs: Organizations need to streamline ADC lifecycle tasks to reduce dependency on specialized expertise and minimize operational overhead. There is a pressing need for tools that can facilitate efficient and agile management of ADC services, ensuring that operations are not hindered by manual processes. Compatibility with various orchestration tools and cloud platforms is essential to support self-service capabilities and enhance operational agility. Ultimately, these needs must be addressed to enable organizations to respond swiftly to changing demands and maintain cost-effective operations.

Confronting ADC Challenges in Dynamic Kubernetes Environments

Modern applications are rapidly evolving to operate within containers, utilizing an architecture that breaks the application into numerous microservices. Each microservice can spin up or scale down as needed, making development and deployment highly efficient. This results in a highly dynamic application environment, where ADC services must continuously adapt to application changes.

Challenges: Native ADCs in Kubernetes containers are often too basic and limited in their ability to expose services to the outside world. They lack advanced capabilities such as application protection, analytics, and cross-container load balancing. Additionally, they are inefficient in processing SSL encryption and decryption.

Needs: To address these limitations, there is a need to complement the native Kubernetes load balancer with an external ADC. This external ADC must understand how to route traffic to each component within the Kubernetes container and continuously adjust its configuration to adapt to the dynamic nature of applications and services. Furthermore, advanced ADC services such as SSL offloading, application protection, and GSLB (global server load balancing) are essential for applications deployed in Kubernetes environments.

Enabling Efficiency and Cost Savings with Modern ADC Solutions

The adoption of cloud technology focuses on higher agility and cost efficiency. However, most organizations now operate across multiple public clouds, private clouds, and datacenter environments. The traditional rigid ADC licensing model per appliance or virtual appliance is no longer viable in this dynamic landscape.

Modern ADC services must be able to seamlessly migrate between environments and scale up or down without concerns about incorrect license sizes. Application protection services integrated into these ADCs must offer the same agility and flexibility.

Today's deployment model should not restrict you to specific environments or capacities. Instead, it should allow dynamic changes to ADC deployment parameters without the need to repurchase licenses. This ensures optimal utilization of ADC functionality and capacity for any deployment scenario throughout the solution's lifecycle.

Summary

The legacy ADC paradigm faces a wide variety of challenges in adapting to the evolving needs of modern applications and simplified operations. These include the complexity of multi-cloud operations, evolving threat landscapes, outdated access management systems, and the lack of actionable SLA visibility. The transition to Kubernetes-based applications requires a complete shift in the ADC design paradigm to provide advanced ADC services in an environment designed for microservices. It's obvious that addressing these challenges requires modern ADC solutions that offer agility and advanced protection while simplifying operations. What are the key considerations when designing such a modern ADC solution to address all these challenges? This question deserves a paper of its own.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.