Web applications are no longer static publishing vehicles. They now routinely process everything from base-level password authentication to sensitive personal information in areas like health care and financial transactions, which makes them an attractive attack surface.

That attack surface is growing. According to an exclusive new survey of IT and business professionals by Network World (NW), 62% of respondents say they expect traffic to their external-facing Web applications to increase during the coming year—traffic that is less predictable, more diverse and more complex.

“Web applications today are the lifeblood of organizations,” said Morgan Gerhart, senior director, products, at Citrix. “In many organizations, they are as critical and sensitive as an ATM is to a bank.”

Given this, it is no wonder that capabilities around security and compliance are critical elements of network function. For example, 48% of survey respondents say source IP preservation is a critical function of a load balancer, and 42% say connection logging is important.

That’s because so many Web applications are subject to regulatory compliance. “They are subject to further scrutiny,” said Gerhart, “so organizations are relying upon the underlying infrastructure to provide a set of services for those applications to stand up in the face of that scrutiny.”

“Today, a bunch of things need to be done from a compliance perspective, in terms of retaining auditability and accountability around who is doing what within a Web application,” Gerhart said.

The problem—and the solution

And that exposes a problem: Most load balancers were never designed to handle such multiple, complex tasks. Many can’t provide such capabilities at all. And some that do, suffer from significant performance degradation when configured to perform the filtering, security and compliance functions demanded by current Web applications. That has led to difficulties with network and server performance, and ultimately affects the end-user experience.

The solution to closing the functionality gap lies in the application delivery controller (ADC), a tool that can handle those diverse demands and provide better security. (For a look at its multiple capabilities, see sidebar: ADCs—better than load balancers. Let us count the ways.)

Even with those benefits, however, the Network-World survey finds that nearly 40% of respondents are only somewhat familiar with ADCs, or not familiar at all.

When evaluating ADCs, the majority of respondents (74%) consider it important that performance levels can be maintained when scaling multi-tenant/multi-instance configurations.

![Pie chart showing performance levels when scaling multi-tenant/multi-instance configurations](chart.png)
ADCs—better than load balancers. Let us count the ways

An application delivery controller (ADC) can:

■ **Maintain performance of Web-based applications that deliver mission-critical functionality, even when scaling multi-tenant/multi-instance configurations.** An ADC can make more intelligent decisions about routing traffic and enhance application server performance by offloading or compressing many compute-intensive tasks.

Those performance enhancement features include:

- **SSL offload and acceleration:** The ADC moves encryption and authentication of SSL requests to a separate device designed for that task. That device also improves security.
- **HTTP compression:** Reduces data to be transferred for HTTP objects through the use of compression tools available in all modern Web browsers.
- **HTTP caching:** Stores static content so that some requests can be handled without contacting the Web servers.
- **TCP offload/buffering:** Consolidates multiple HTTP requests from multiple clients into a single TCP socket to the back-end servers.

- **DNS load balancing:** Hands off traffic to Web servers based on the health of each, which geographic region it serves and the percentage of traffic it should receive.
- **Clustering:** Allows multiple appliances, physical or virtual, to work in unison to deliver one or more applications. The ADC cluster appears as a single virtual IP address.

■ **Provide security threat protection.** ADCs offer the following security and compliance benefits lacking in traditional load balancers:

- **Source IP preservation:** Meets compliance regulations that require auditability and accountability around who is doing what within a Web application.
- **Connection logging:** Monitors the handling of sensitive customer information.
- **Content filtering:** Provides intelligent modification of traffic and improved security.
- **Web Application Firewall**

The case for Citrix NetScaler

The unfamiliarity with ADCs makes it crucial to understand the options on the market. According to multiple findings, the Citrix NetScaler ADC is well ahead of the competition.

A March 2014 evaluation by the Tolly Group of several common configurations of NetScaler with comparable products from the F5 Networks BIG-IP line of ADC solutions found that NetScaler ADCs deliver “up to 4.8 times the performance (plus) more consistent performance as more features are added.”

Kevin Tolly, founder of the Tolly Group, said another advantage for customers is that, “rather than make them pay for expensive proprietary silicon to deliver advanced performance...”
functionality, Citrix NetScaler leverages the Intel processor ecosystem to deliver performance that exceeds that of proprietary silicon,” at an affordable price.

Another benefit is so-called “active-active” clustering, which is far superior to “active-passive” pairs, since multiple ADCs share the load and take up the slack if one of them drops offline.

NetScaler’s users are just as enthused. Dan Drysdale, director of strategic architecture services for Centene, a health care services provider, said the company’s data center was struggling with performance problems and high support costs in 2011 when it turned to NetScaler MPX with High Availability (HA).

Drysdale said the configuration improved performance by 25%, cut its capital and operating expenses by 20% and reduced support costs as well, since one employee can now handle what previously required six networking employees.

Bruce Perrin, COO and acting CIO at Phenix Energy Group, an oil pipeline and construction company, tells a similar story. After nearly two years of intense research, “we found the NetScaler to be easier to configure, manage and reconfigure,” he said.

“We also found its interface to be clear and unambiguous,” he added. “One of our most important issues was efficient use of bandwidth both within and between data centers. One of the most telling arguments in favor of NetScaler was Cisco’s abandonment of the market and adoption of NetScaler as their favored ADC to replace it.”

The unfamiliarity with ADCs makes it crucial to understand the options on the market. According to multiple findings, the Citrix NetScaler ADC is well ahead of the competition.

FOR MORE INFORMATION, please visit: www.citrix.com/netscaler