How to Future-Proof Application Delivery

The new requirements for application delivery mean adopting the principles behind cloud, DevOps, and SDN, and enabling emerging security models. It's no longer just meeting the goal of fast, secure, and available—now you must also provision apps in minutes instead of months, and with significantly reduced operational costs.

White Paper

by Lori MacVittie

Introduction

Enterprises today are under incredible pressure to do what sounds impossible: transform the data center into an agile, efficient application delivery machine while simultaneously cutting costs. With estimates putting the cost of keeping the lights on ranging from 72% (Forrester)[1] to 80% (North Bridge Ventures)[2] of the entire IT budget, there isn't a lot left with which IT leaders can work to meet this demand.

One of the ways organizations can begin to execute on this mission is to look at the heart of the data center—at its application delivery strategy. Application delivery comprises a wide variety of services spanning security, mobility, identity and access, performance, and availability. These critical services protect and enhance applications as they traverse the paths between consumers, customers, employees, and partners.

Many of these services are delivered by an Application Delivery Controller (ADC). This makes the ADC a critical component in any data center transformation strategy because it directly affects the security, reliability, and performance of applications, as well as the operational costs associated with getting those applications to market quickly.

That means your choice of an ADC is a strategic one that warrants serious consideration if you're going to deliver applications today while paving the way to deliver the applications of tomorrow. Ninety-five percent of C-level executives expect their company to be using the IoT in three years' time[4]—which means supporting another explosion of applications needed to license and manage these sometimes- and always-connected things. And while it's important to architect a strategic, future-enabling network, it can't disrupt existing, business critical applications.

Traditional datasheet criteria of speeds and feeds are insufficient for modern applications that may reside on premises or in the cloud—or both. In the real world, organizations must consider not only technical specifications, but operations as well as alignment with data center and business initiatives that rely heavily on applications delivered by the ADC.

The new requirements for application delivery are not just about bandwidth and throughput. They are also about deployment velocity and operational efficiency, and the ability to tailor delivery mechanisms to the unique needs of hundreds of different applications that support the consumers and employees who interact with them on many devices and in many locations.

Business and Technology Objectives Align

Top Business Objectives

- Decrease operation costs (54%)
- Increase worker productivity (44%)

Top Technology Objectives

- Lower IT operation costs by consolidation/simplification (55%)
- Boost end-user workforce productivity (43%)[3]

There are four key categories to consider when choosing an ADC to support a strategic application delivery approach rather than as a tactical means to address a specific application delivery challenge:

- Cloud capabilities
- Programmability
- Scalability
- Security

Cloud Capabilities

Managing applications is much more complex today than it was just five years ago. On the back end, applications can now reside anywhere, whether on premises or in the cloud or both. Apps may be SaaS or composed of microservices, based on APIs or delivered via traditional application architectures. In all cases, apps need services to ensure reliability, security, and optimal performance. Cloud computing in all its forms remains a trend—one that has a significant impact on data center strategy according to a survey of 300 top F5 customers, placing as three of the top four technologies.[5]

Being able to connect to a cloud using solutions based on traditional network bridging technologies is just the first step. Deploying operationally consistent application services across on-premises and cloud environments is the next. That means supporting a comprehensive set of cloud management platforms such as OpenStack and VMware vCHS, as well as being deployable on all the various hypervisors upon which various cloud computing environments are based. Whether running in AWS, KVM, Citrix Xen, VMware, or Microsoft Hyper-V environments, F5 virtual editions support all F5 application services, from identity and access management to security, mobility, availability, and performance.

But even that is not enough to support today's hybrid cloud architectures and enable migration and deployment into the future. It's also critical to have the means to automate, orchestrate, and manage services whether they reside on-premises or in the cloud, as well as the depth and breadth to which those capabilities support an application focus. Whether looking at APIs or management capabilities, an ADC should provide the means by which the services applications need can be holistically provisioned and managed from the perspective of the application, not the individual services. F5 iApps, which are executable application service templates, and BIG-IQ, F5's intelligent service orchestration platform, are both application-driven. This gives app owners and administrators the ability to programmatically define provisioning and management of all the application services needed to deliver the application.

> "F5 provides us with added network capacity, improved scalability, and greater security in a single solution that is easy and cost effective to operate.
>
> —Gonen Wilf, Head of Production, LivePerson

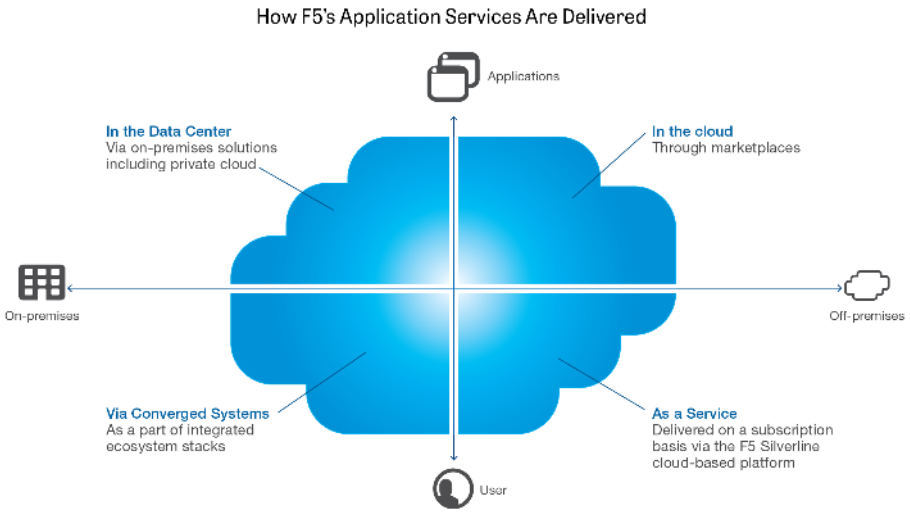


Figure 1: F5 can help organizations create, connect, and consume services anywhere in a hybrid cloud architecture.

Finally, when considering an ADC it is important to measure the flexiblity in how services are consumed. On premises and in the cloud are only two of the options. A third option—as a Service—is rapidly emerging in response to security concerns raised by the unique needs of BYOD 2.0, explosive device proliferation, and the increasing threat from DDoS attacks.

F5 believes the future of hybrid cloud includes a seamless, hybrid approach to delivering services—particularly those that interact with clients both to protect them and defend against them. Services such as web anti-fraud are a critical component in ensuring organizations can take advantage of the mobile app economy while preventing consumers and employees from falling prey to attackers. Likewise, DDoS mitigation as a service enables organizations to extend their security perimeters on-demand, in the face of an attack, preventing the overwhelming costs of continuous DDoS mitigation as a service without sacrificing the ability to prevent a sudden attack from oversubscribing network connectivity. A forward-looking, future-enabling ADC will offer both traditional, on-premises protection, as well as cloud-based protections to provide the most cost-effective, efficient means of protecting apps, networks, and consumers.

Scalability

Scalability is the property of an application delivery system to scale itself and the applications it delivers. In the past, this has been measured solely based on speeds and feeds. More recently, virtual density has been introduced as a metric by which to determine an ADC's ability to scale. But in an age where operational scalability is just as critical to IT supporting an expanding base of devices, users, and applications, it is no longer the only measure. Operational scale must also be considered as it ensures that operations can deploy and manage a hundred apps as efficiently as one. When considering the choice of an ADC to support existing and future apps and architectures, carefully evaluate both infrastructure and operational scalability to ensure cost-effectiveness across both.

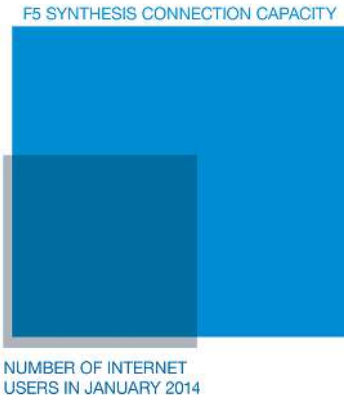
Infrastructure Scalability

ScaleN is an F5 technology that uses horizontal clustering, virtualization, and on-demand scaling capabilities to enable more efficient, elastic, and multi-tenant solutions for data centers, clouds, and hybrid deployments. ScaleN breaks away from traditional infrastructure limitations and offers multiple scalability and consolidation models to help organizations meet their specific business needs.

F5's unique ScaleN architecture redefined the concept of active-active scalability at both the infrastructure and application layers. In particular, ScaleN introduced the concept of application clustering: the ability to isolate applications and provide high availability and scale for a single application across multiple application delivery systems in a multi-tenant-friendly paradigm. Unlike competing approaches, ScaleN is non-disruptive and does not require significant re-architecture of the application delivery tier to implement.

The F5 Synthesis high-performance services fabric can respond to 471 million DNS queries per second. At that rate, it would take 2 seconds to resolve the IP addresses for each of the 861 million sites that make up the Internet today.[6]

With F5 Synthesis, a services fabric can be provisioned and managed whether on-premises or in the cloud from the BIG-IQ unified management platform. BIG-IQ enables network engineers, operators, security professionals, and app owners to manage the services fabric from their own unique perspective using a modular approach that supports the division of responsibility across IT groups. This allows app owners to manage apps and services while network engineers and operators manage at the fabric and ADC layers.



Operational Scale

The complexity inherent in today's data center networks is inarguably one of the drivers of software-defined architectures (cloud, SDDC, and SDN) as well as movements like DevOps. For years now we've added applications and services, and responded to new threats and requirements from the business with new boxes and new capabilities. All of them cobbled together using traditional networking principles that adhere to providing reliability and scale through redundancy. The result is complex, hard to manage, and notably inflexible. It doesn't scale from an operational perspective.

ADC consolidation is a tactical means of addressing this complexity and lack of scalability. Its goal is to reduce the number of ADCs in the data center. F5 certainly supports such a tactic. A single F5 VIPRION 4800 can support 80 multi-tenant instances. With up to 32 devices in an F5 Synthesis services fabric, that means 2560 individual instances—more than suitable for consolidation efforts.

What this approach misses is the more strategic means of achieving operational scale: standardization. Standardizing on a single services platform for a broader set of application services achieves operational efficiency not only through reducing the physical number of devices in the data center, but by reducing the variety of devices as well. Reducing variation through standardization is a key principal of modern and emerging data center technologies such as SDN, SDDC, and cloud computing.

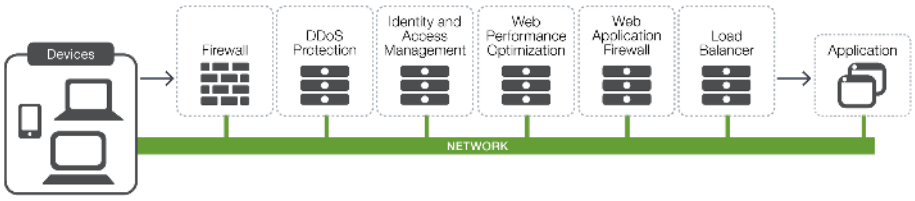


Figure 2: Traditional tactical deployment of individual application services.

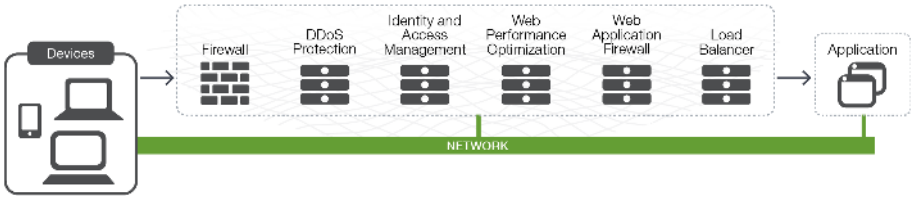
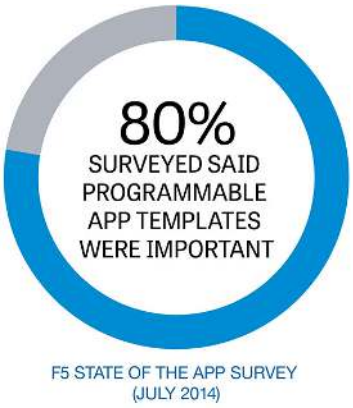


Figure 3: F5 Synthesis strategic, platform-based deployment of application services.

F5 Synthesis builds on an application services platform, not a product. This means as new services are introduced, they can be deployed on the same standardized platform. Standardizing on a platform means you can choose from a comprehensive range of application services without adding the management complexity and disruptions that come with implementing single-purpose appliances. Standardization "can reduce the support and operations cost associated with the IT landscape, and the impact can be dramatic."[7]

Programmability

Programmability is at the heart of the next-generation data center, driven by software-defined architectures. These transformational technologies and methodologies—SDN, SDDC, cloud, and DevOps—are having a significant effect on the way in which the entire network is designed and operates. Programmability is both the ability to manage devices and services via a standards-based API, and the ability to programmatically interact with data traversing the data plane.



F5 began its support for programmability in 2003 by separating its control and data planes and providing both a programmatic API for integration and automation (iControl) as well as participating in the data path (the iRules scripting language). F5 has continued to embrace and extend the principles of programmability now associated with DevOps and SDN with years of integration with partners (Cisco, VMware, Microsoft, Cenzic, WhiteHat, IBM, Oracle) as well as customers.

Additionally, F5 has advanced the notion of programmatic control with its automation framework, iApps. Comprising repeatable, programmable, and re-entrant templates, iApps encapsulates best practices into an executable script that can reduce the time to configure and deploy application network services from weeks to minutes. Like all F5 programmable components, iApps are supported by the DevCentral community, with both community- and F5-supported iApps available.

Additionally, only F5 offers the flexibility and extensibility of iRules, a data-plane scripting language designed to allow interaction and participation of traffic on the data plane. Data path programmability enables organizations to tailor services to meet their unique business and application requirements. Turnkey services assume every app and every process is the same when the reality is operational processes—like business processes—can provide a competitive advantage when able to support custom logic and processing. With an active, robust ecosystem of developers and engineers supporting thousands of iRules, the F5 BIG-IP platform can mitigate zero-day security threats, support new or custom application protocols, and address application issues with equal alacrity.

Lastly, recognizing that SDN, like cloud, will certainly have an impact on future data center architectures, F5 is collaborating with network fabric SDN providers such as Cisco and BigSwitch to enable integration and interoperability with SDN-related protocols and transitory architectures.

Security

The breadth and depth of ongoing attacks against organizations of all sizes is resulting in a security renaissance. There is a growing awareness and understanding of the importance of securing not just the network, but infrastructure and applications as well. It's no longer enough to simply drop packets.

Attackers are increasingly moving up the stack, to the application layers where they can exploit protocols and behavior with increasing success. Conventional firewalls are beginning to show their limitations in detecting and repelling modern attacks, and in protecting cloud-based apps and mobile users. The ability to inspect not only content, but sessions, and interpret user behavior is critical to defending against attacks designed to consume resources to affect denial of service to legitimate customers.

> The sophisticated authentication process we achieved with F5 [iRules] helped us eliminate immeasurable risk to our users and our business.
>
> —Simon Blackstein, Corporate IT Infrastructure, Facebook

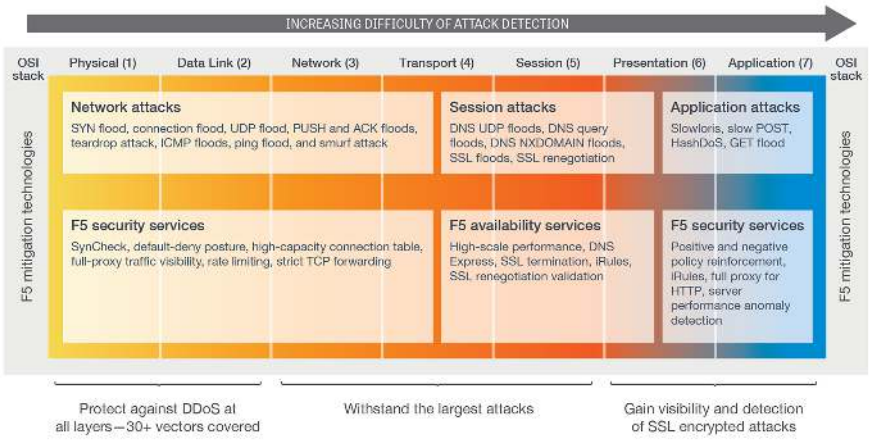


Figure 4: F5 mitigation technologies protect applications at every layer of the stack.

The introduction of mobility and cloud computing has made it even more necessary to take a fresh look at what we consider the enterprise perimeter. IP-based security technologies are no longer able to adequately supply protection against attacks that may be targeting employee devices and applications located outside the corporate network. A strategic approach to access and security services requires the ability to act on ID rather than IP. This capability is critical to the success of cloud- and mobility-related initiatives. The capacity of these services to hyper-scale across the data center and cloud applications is required to ensure cost-effective access management as the impact of mobility and the Internet of Things continue to drive the number of users needing access higher and higher.

F5 continues to push the envelope—and the reach of the enterprise perimeter—with advanced firewall services, identity and access control, and cloud-based mobility and DDoS protection services. With a platform that provides a unified view of layers 3 through 7 for both general and ICSA-required reporting and alerts, as well as integration with SIEM vendors, F5's security services enable organizations to combine traditional on-premises and cloud-based security services to build a new security architecture based on the application intelligence of F5's platform.

Conclusion

Trends such as BYOD, cloud, SDN, virtualization, and highly demanding customers are focusing a variety of requirements on application delivery systems both in the data center and in cloud computing environments. These transitions are pushing ADCs to be more than simple load balancers, and even more than "simple advanced" ADCs: today's data center demands an intelligent platform that can handle all application delivery needs in one context.

F5 Synthesis is capable of managing every delivery aspect of users, applications, systems, and infrastructure, and is an integral part of an elastic, dynamic infrastructure designed to support these requirements. Scalability, performance, and security have always been important to end-user satisfaction and meeting business and operational requirements, but it is increasingly the case that delivery infrastructure must do so while adapting to new data center and network models that encourage efficiency, automation, and orchestration.

---

1 http://www.computerworld.com/s/article/9243312/How_to_balance_maintenance_and_IT_innovation

2 http://www.slideshare.net/mjskok/2014-future-of-cloud-computing-4th-annual-survey-results

3 http://www.networkworld.com/article/2359344/data-center/155583-Network-Worlds-2014-State-of-the-Network-survey.html

4 http://www.arm.com/files/pdf/eiu_internet_business_index_web.pdf

5 F5 State of the App Survey, July 2014.

6 http://news.netcraft.com/archives/2014/07/31/july-2014-web-server-survey.html

7 http://www.asugnews.com/article/monday-metric-benefits-of-it-standardization (2013)

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com