White Paper
BIG-IP Virtual Edition for Microsoft Azure

F5 BIG-IP and Microsoft Azure

A Seamless Path to the Hybrid Cloud

Companies are increasingly drawn to public cloud services because of their promise of increased efficiency and scalability. However, lingering concerns surrounding security and the lack of robust application and networking services are keeping many enterprises from modernizing data center strategies with a hybrid cloud architecture.

Shifting workloads to public clouds such as Microsoft Azure delivers several benefits, from reducing overall operational costs to providing greater flexibility in systems deployment. By integrating public cloud resources as part of a global enterprise computing architecture, organizations can boost data center agility and realize easy, on-demand resource elasticity—both essential for today's peak business cycles—without the burden of a costly up-front investment.

Because of the potential upside of cloud services, momentum behind their adoption is mounting. Gartner predicts that companies will invest $240 billion in cloud services by 2017[1], and a recent Algosec survey shows an uptick in organizations committed to making public cloud platforms a critical piece of their enterprise strategies. Seventy percent of the respondents to the Algosec survey said they plan to deploy 10 percent to 60 percent of their business applications on public infrastructure as a service (IaaS) platforms within the next three years[2].

Yet for all the momentum behind the public cloud, there are challenges for enterprises trying to seamlessly bridge IaaS and platform as a service (PaaS) workloads and existing on-premises environments. Complying with security policies, managing diverse technologies and having the ability to achieve scalability while hitting acceptable performance targets for critical Tier 1 applications are among the chief enterprise concerns.

These issues—especially consistency of service—are being readily addressed.

Gartner predicts that companies will invest $240 billion in cloud services by 2017

[1] "The Cheap, Convenient Cloud," The Economist, April 18,2015; http://www.economist.com/news/business/21648685-cloud-computing-prices-keep-falling-whole-it-business-will-change-cheap-convenient

[2] "Five Predictions for Hybrid Cloud Environments in 2015," IT Business Edge; http://www.itbusinessedge.com/slideshows/five-predictions-for-hybrid-cloud-environments-in-2015-02.html

Microsoft has made significant investments in developing Azure, a leading secure public cloud environment that supports the full range of globally recognized regulatory compliance standards and has been adopted by 80 percent of Fortune 500 companies. Add F5's BIG-IP Virtual Edition (VE) for Microsoft Azure into the mix, and companies can easily make a seamless transition to a hybrid cloud architecture and still retain a uniform level of network control, application services and performance optimization, regardless of whether services are running on the public cloud or a private cloud in a corporate data center.

Hybrid Cloud Without the Learning Curve

BIG-IP VE for Microsoft Azure enables consistent application delivery throughout an organization's internal data centers and that organization's evolving hybrid cloud architectures. The key lies in the programmability across the data, control and management planes that F5's Traffic Management Operating System (TMOS) offers, bringing advanced application and networking services to Microsoft Azure without requiring IT to get up to speed on a new management platform.

In addition, BIG-IP VE for Microsoft Azure delivers the full spectrum of familiar BIG-IP modules offered by BIG-IP appliances in concert with the same user interface and support for F5 iRules, an event-driven scripting language, and F5 iApps, a user-customizable framework for deploying applications. For example, BIG-IP VE for Microsoft Azure features the same F5 robust traffic management, DNS services and SSL offload and termination capabilities as the physical appliances. BIG-IP Local Traffic Manager, used to optimize network infrastructure to meet availability, security and performance requirements for critical business applications, makes it easy for IT organizations to monitor and dynamically respond to network traffic. The complete DNS security features incorporated in the BIG-IP VE stack protect infrastructure from the latest threat vectors.

From there, BIG-IP VE for Microsoft Azure addresses application security in other ways. The platform's Application Security Manager (ASM) provides protection against the Open Web Application Security Project's top 10 threats, application vulnerabilities and zero-day attacks. In addition, BIG-IP VE's Web Application Firewall (WAF) offers leading Layer 4-7 DDoS defenses, virtual patching and granular attack visibility designed to ward off the most-sophisticated threats, and the platform is also stocked with antimalware and antifraud services, ensuring compliance with key regulatory standards such as HIPAA and PCI DSS.

> An on-premises physical BIG-IP appliance can provide a secure IPsec VPN tunnel and additional load balancing capabilities.

For an additional layer of protection against malicious traffic, BIG-IP VE for Microsoft Azure features F5's IP Intelligence Services, a solution that provides richer IP intelligence and stronger, context-based security, helping organizations protect their applications and brands while avoiding costly compliance penalties. Single-sign-on and multifactor authentication capabilities, available through BIG-IP Access Policy Manager (APM), provide more-granular security controls based on user identity and context.

Deploying BIG-IP VE for Microsoft Azure

BIG-IP VE for Microsoft Azure can be deployed in a variety of scenarios. Here are a few sample use cases:

Deployed in the cloud with single sign-on and firewall. This provides the strongest security footprint for applications hosted entirely in Azure. BIG-IP APM sits between the applications and users to serve as a strategic control point in the network. Its role here is to protect public-facing applications with policy-based, context-aware access for external users as well as delivering additional application and network security via Big-IP ASM and BIG-IP Advanced Firewall Manager (AFM).

Deployed in a hybrid cloud. A hybrid architecture is proving to be the most common among enterprises. The idea here is to host sensitive customer data in on-premises clouds while leveraging the public Azure cloud to host the application front end and to supplement computing resources during peak traffic periods. A sample configuration of this use case deploys multiple BIG-IP VEs for Microsoft Azure to handle web server load balancing, authentication services and security through a web application firewall. An on-premises physical BIG-IP appliance can provide a secure IPsec VPN tunnel and additional load balancing capabilities.

Deployed in a hybrid cloud across regions with global load balancing and federation. The public cloud enables organizations to deliver applications from multiple locations across different geographic regions as a means of boosting performance and providing failover capabilities in the event of a problem in one particular region. BIG-IP VE for Microsoft Azure fosters those advantages by balancing traffic between on-premises data centers and Azure clouds in the United States and Europe, for example. At the same time, BIG-IP AFM and BIG-IP ASM deliver network and application security across those respective environments.

The path to the public cloud is clear. With F5's BIG-IP VE for Microsoft Azure, companies can reap the scalability and cost benefits of a hybrid data center architecture without the unknowns of starting from scratch. At the same time, they get all the consistency of service benefits associated with a proven environment.

To learn more about BIG-IP VE for Microsoft Azure and the F5 and Microsoft partnership, go to f5.com/microsoft.