PARTNER USE CASE

F5 and Secure Windows Azure Access

F5 technologies give enterprises a new way to provide secure remote access and traffic management within their Windows Azure infrastructure.

Ryan Korock, F5 Networks

Contents

Introduction

For nearly two decades, enterprises have relied on F5 in the data center to provide intelligence and sophistication in the network to complement commonly deployed advanced server applications. With the modern F5® TMOS® traffic management engine, an operating system built from the ground up for application delivery on the F5 BIG-IP® platform, data centers have achieved unparalleled levels of scalability, performance, and security by taking advantage of an often overlooked resource: the network. As enterprises look to expand to the public cloud, they must ensure that the same level of network intelligence and control they achieve with F5 in the local data center can be extended into the cloud.

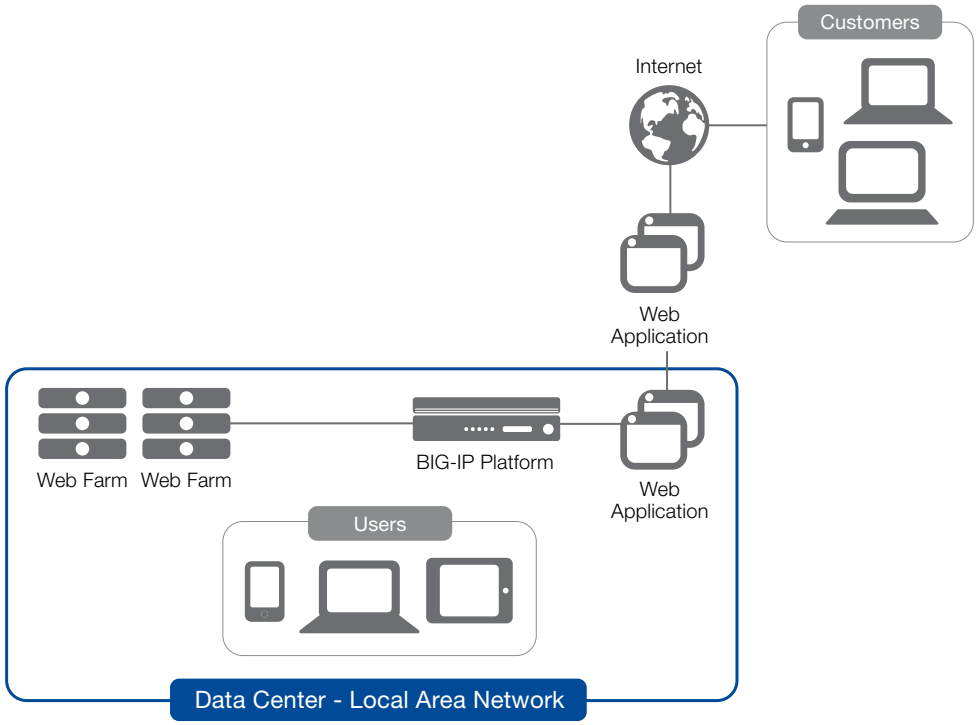

Figure 1: Traditional data center configuration using the BIG-IP platform for advanced traffic management.

These same enterprises have recently begun to blur the traditional boundaries of the data center by extending local workloads into the Windows Azure public cloud. With Azure, you can take advantage of the resiliency and scale efficiencies that can only be offered by a public cloud, and F5 expands on these capabilities by enabling you to secure and manage the traffic between on-premises data centers and the cloud via the network.

Expanding into Windows Azure

Most enterprises looking to host workloads in Windows Azure are discovering that a hybrid approach allows them to reap the benefits of the public cloud, while also keeping sensitive data within the confines of the corporate data center. The hybrid model, with workloads hosted both locally and within the Azure cloud, provides the foundation for you to manage costs, achieve the desired resiliency, and comply with data regulations. You can extend these benefits by leveraging the native traffic management and security features of the F5 BIG-IP platform.

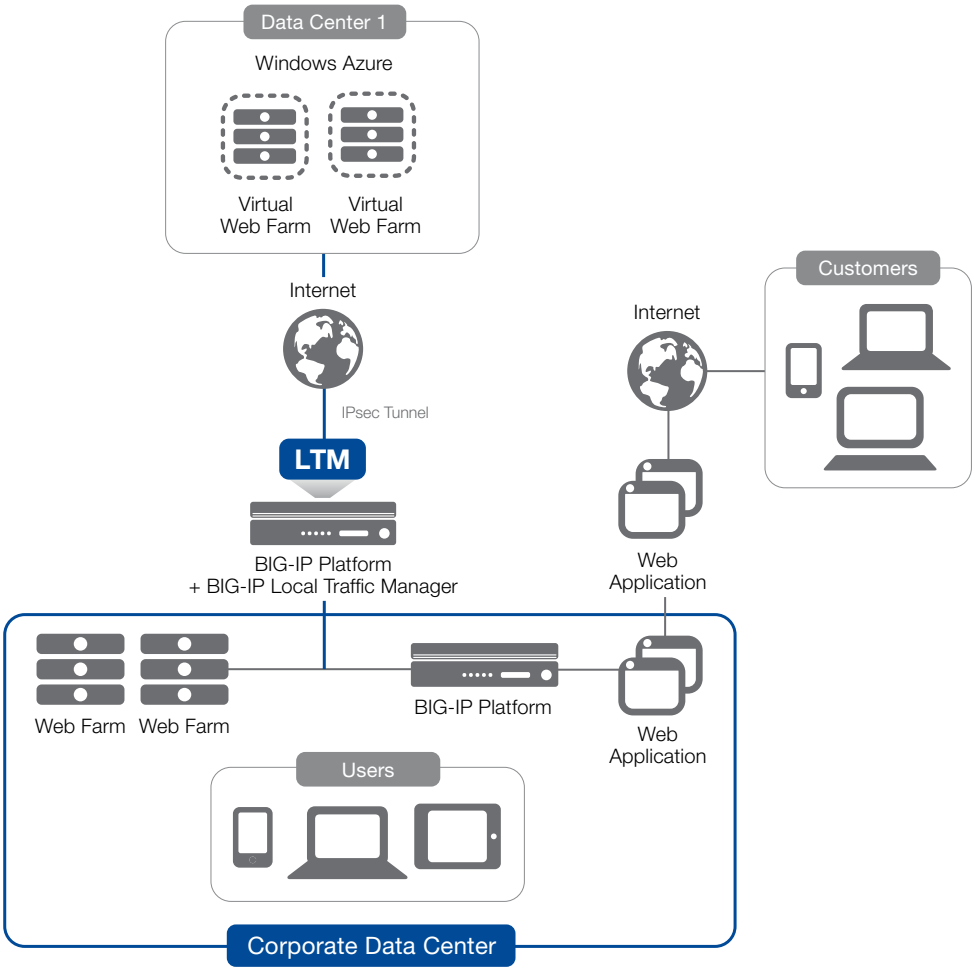

Figure 2: You can establish a secure IPsec tunnel between your corporate data center and Windows Azure using the BIG-IP platform.

Azure Secure Tunneling

Hybrid deployments are most successful when the Azure cloud is deployed as an extension of the corporate data center, rather than as a separate data center. But to achieve this, you need secure and seamless connectivity between the two data centers. F5 BIG-IP® Local Traffic Manager™ (LTM), which has an advanced IPsec engine built into its core traffic management engine, can bridge the corporate and Azure networks by creating a secure tunnel and routing between them as if they were connected by the same local fabric.

Traffic Management in the Azure Cloud

With resources active in your local data center and in the cloud, and costs accruing differently for each, you can use Azure most cost-effectively by managing network traffic appropriately. Sometimes it may make sense to keep all traffic in the corporate data center until bursting is necessary; or maybe you need to load balance traffic concurrently amongst the server farm split across the Azure cloud and local data centers. BIG-IP LTM seamlessly manages this traffic between Azure and the local data center—minimizing costs and maximizing availability and performance.

Managing Multi-Cloud Environments

With multiple geographically dispersed Azure data centers over which to spread the network workload, you could leverage Azure for site resiliency. To realize this potential, you can use the intelligence and network management engine in BIG-IP LTM. Not only is a single instance of BIG-IP LTM capable of supporting IPsec tunnels to multiple Azure clouds, but more important, it can intelligently manage the traffic to each virtual network, whether local or remote. BIG-IP LTM can split traffic to multiple Azure clouds based on end-to-end performance of each specific user, and based on availability, cost, or specific workload. And with the F5 iRules® scripting language, you can split, isolate, or load balance traffic based on almost any criteria.

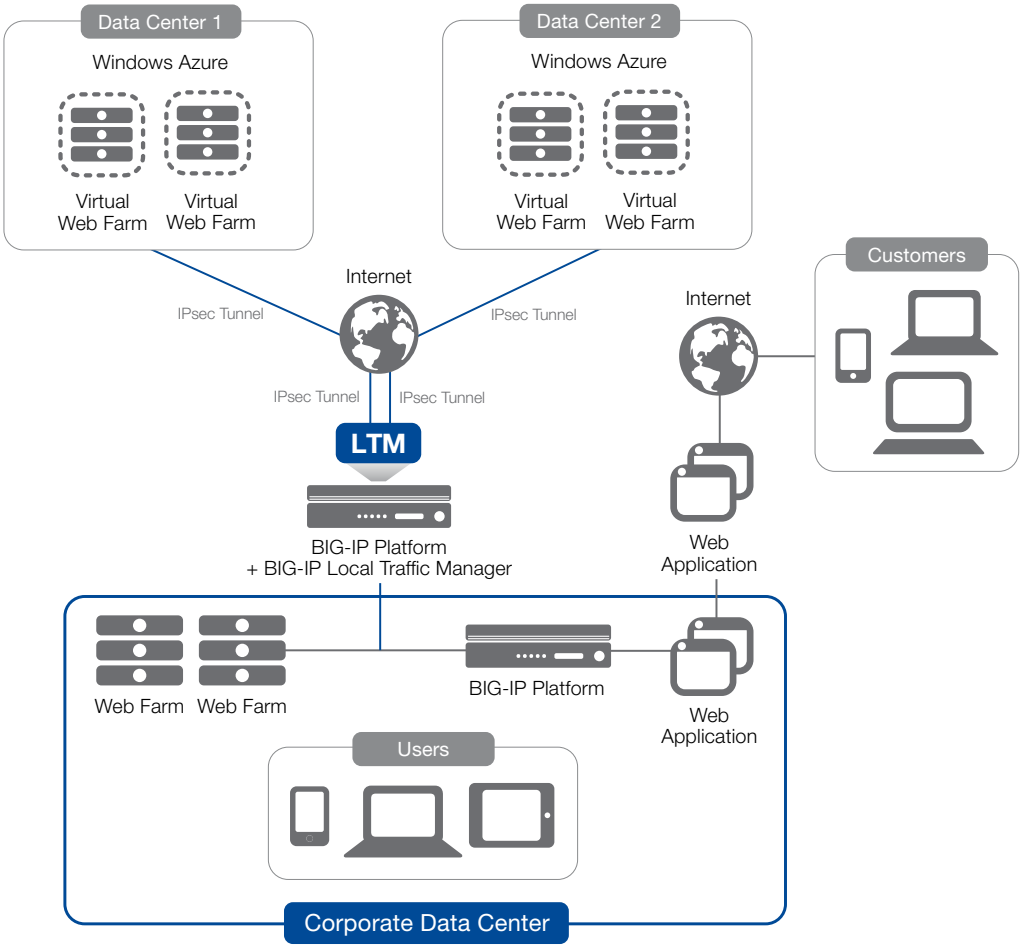

Figure 3: A single instance of BIG-IP LTM can manage secure tunnels to multiple Azure endpoints.

Performance, Security, and Redundancy

For enterprises that want to take full advantage of their cloud investment, creating the tunnel from the data center to the Azure cloud(s) is just part of the solution; even more critical is making sure that the tunnels are optimized, secure, and fault tolerant. When enterprises configure BIG-IP LTM as the gateway to the Azure cloud, it will negotiate an IPsec connection using industry-leading encryption at near wire speed. BIG-IP LTM's network awareness means it can determine when to enable WAN acceleration features as it sends users to remote Azure clouds. And with most F5 gear deployed as

redundant pairs, the BIG-IP devices can be configured as tunnel backups for each other. As soon as a failover occurs, the newly activated device will establish a new IPsec tunnel with Azure, minimizing any disruption of service.

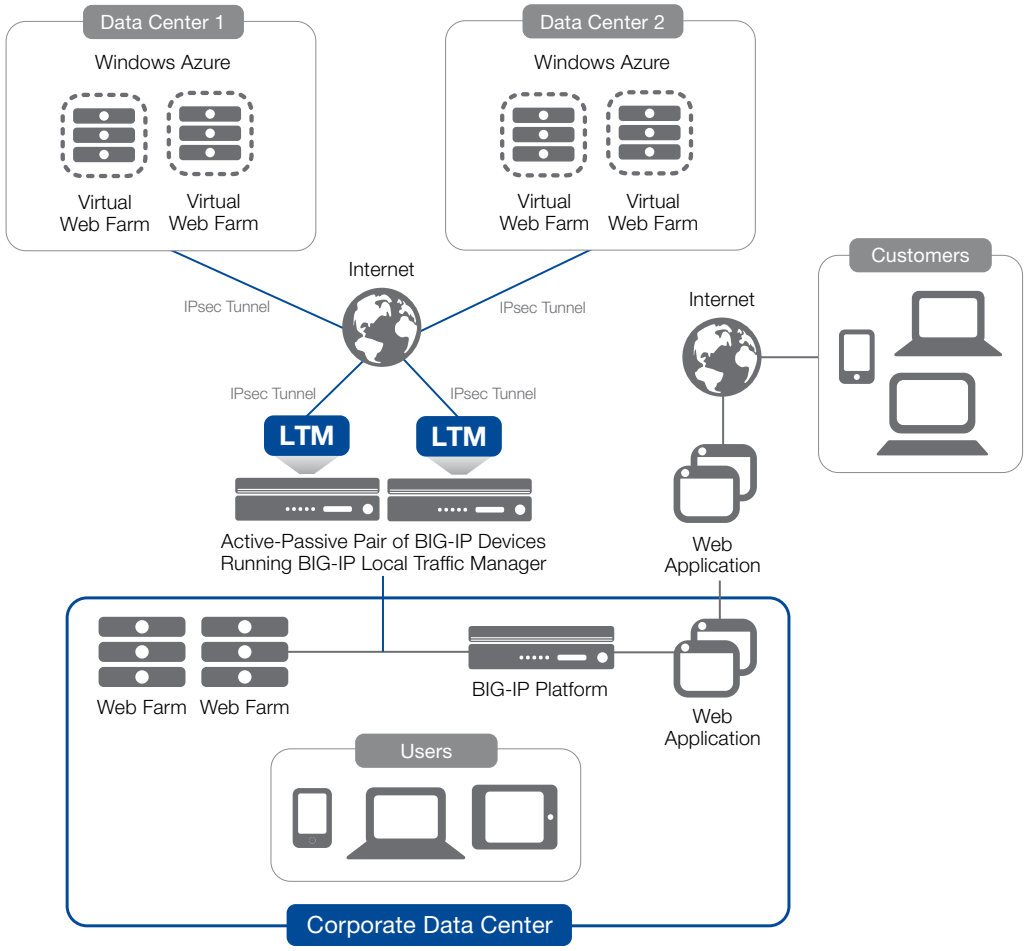

Figure 4: An active-passive pair of BIG-IP devices eliminates the possibility of service disruption.

Conclusion

With a rich hosting toolset available for enterprises to take advantage of, Azure has quickly evolved into a system that enterprises can rely on to manage their business-critical workloads. By having F5 manage the network between the local data center and the Azure clouds, the benefits of Azure increase rapidly and dramatically. With the ability to define traffic preferences, awareness of the health and availability of both the local and remote workloads, and FIPS-level strength encryption standards, you can count on the F5 solution to direct users to the local or remote resources with performance, cost, and security in mind.

Learn More

To find technical details and deployment configuration guidance, visit DevCentral™, F5's user community of 120,000+ members; you can also visit f5.com/microsoft.

You can also contact msfttechteam@f5.com anytime for more information.

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com