F5 and VMware SDDC

SOLUTION OVERVIEW

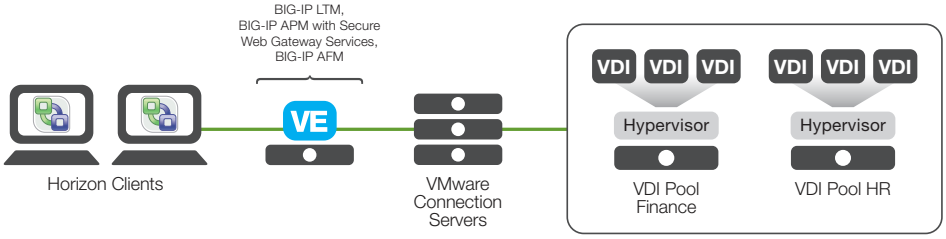
F5 and VMware Offerings

- BIG-IP Local Traffic Manager (LTM) Virtual Edition (VE)
- BIG-IP Access Policy Manager (APM) Virtual Edition
- BIG-IP Advanced Firewall Manager (AFM) Virtual Edition
- F5 Secure Web Gateway Services
- VMware vRealize™ Orchestrator™ (vRO) and BIG-IP vRO Plug-in
- VMware NSX™
- VMware Horizon® 6

Orchestrate Advanced Networking Services for VMware Horizon in the Software-Defined Data Center

The Software-Defined Data Center (SDDC) is one in which all infrastructure is virtualized and delivered as a service. As such, it has the power to transform and streamline infrastructure provisioning and application deployments. Automated, repeatable provisioning of computing resources, networking components, virtual machines, and advanced networking services and security will help to deliver on the promise of the SDDC.

To support this new era of software-defined everything, VMware and F5 are collaborating to ensure that mission-critical applications can dynamically and automatically leverage advanced network services in order to function at peak performance. To do so, a variety of components are necessary in order to provision a secure and available infrastructure that uses network virtualization, management, and automation tools. Together, VMware and F5 solutions enable an elastic VMware Horizon deployment that provides high application performance, scalability and, most importantly, security. This functional environment, which spans the breadth of the VMware and F5 product portfolios, demonstrates the value of advanced networking services.



F5 and VMware components cooperate in an SDDC environment

Benefits of an F5- and VMware-enabled SDDC

Automated provisioning of network, virtual machines, and security policies

Together, F5 and VMware products provide a template architecture for a scalable and secure Horizon environment that includes automated provisioning of networking and compute resources, hardened security, DNS services, improved scalability of virtual desktops, and application availability. This design and implementation should be the blueprint for a hardened virtual desktop design.

Protect corporate assets and information

F5 Secure Web Gateway Services protects the enterprise from outbound browsing security threats and makes it possible to apply distinct security policies to different Horizon user groups. This is especially important for an increasingly mobile workforce that routinely accesses a virtual desktop environment. In addition, firewall policies configured in BIG-IP AFM VE provide the necessary security between virtual desktops and applications, ensuring that unauthorized traffic is not allowed.

Rapid, Automated Network Provisioning and Layer 4-7 Services

Utilizing VMware NSX and the BIG-IP vRO plug-ins in vRO enables rapid provisioning of all elements of the networking stack. This simplifies the overall deployment of the Horizon environment and also ensures a secure, protected environment.

F5 Software-Defined Application Services in Action

The movement to a software-defined data center means that advanced application delivery services can be automatically provisioned and deployed. This is especially important in a Horizon environment as virtual desktop environments often need to scale rapidly due to seasonal business, expansion, or an increasingly mobile workforce. Having the flexibility to adapt to business conditions while protecting critical IT assets is a key part of this combined solution.

Essential Products

The following F5 and VMware products are crucial to orchestrating advanced networking services in an elastic VMware Horizon deployment:

F5® BIG-IP® Local Traffic Manager™ (LTM) Virtual Edition (VE) is a flexible, high-performance application delivery system. With its application-centric perspective, BIG-IP LTM VE optimizes the network infrastructure to deliver availability, security, and performance for critical business applications. BIG-IP LTM enables Horizon desktop deployments to scale by distributing traffic across Horizon connection servers within the data center, enabling single namespace connectivity, SSL offload, and username persistence.

BIG-IP Access Policy Manager® (APM) Virtual Edition protects public-facing applications by providing policy-based, context-aware access for users and by consolidating the access infrastructure. Working with the BIG-IP Edge Client, BIG-IP APM VE provides users secure mobile and remote access to corporate resources such as Microsoft Exchange, Microsoft SharePoint, and VMware Horizon over all types of networks and from virtually any device.

BIG-IP Advanced Firewall Manager™ (AFM) Virtual Edition, in combination with other BIG-IP solutions, enhances security capabilities and eliminates the need for point products that support application delivery, application security, user access control, and DDoS protection. BIG-IP AFM VE also reduces total cost of ownership (TCO) and increases operational efficiencies. In concert with VMware NSX, BIG-IP AFM VE ensures secure communications for both north-south and east-west traffic.

Secure Web Gateway Services. Failures in outbound security can be very costly to the enterprise, whether the result is data loss, which can have a direct financial impact on the business, or declining employee productivity due to inappropriate use of the Internet. While there are many vendors and solutions to choose from for outbound security, F5 offers a superior alternative. Partnering with WebSense, F5 provides Secure Web Gateway Services as a feature of BIG-IP Access Policy Manager. These services address the malware, malicious users, and advanced persistent threats that continue to pervade networked environments.

VMware vRealize Orchestrator (vRO) and BIG-IP vRO Plug-In. VMware vRealize Orchestrator simplifies the automation of complex IT tasks. It integrates with VMware vCloud Suite® components to adapt and extend service delivery and operational management, effectively working with existing infrastructure, tools, and processes. The F5 BIG-IP vRO plug-in enables the orchestration of BIG-IP devices in a virtualized environment.

VMware NSX virtualization platform is helping hundreds of customers realize the full potential of the SDDC. When it comes to networking, NSX provides key networking automation for simplified layer 2 and layer 3 networking. With NSX, enterprises can create, save, delete, and restore virtual networks on demand without reconfiguring the physical network.

VMware Horizon 6 enables organizations to deliver virtual or remote desktops and applications to users through a single virtual desktop infrastructure (VDI) platform.

For more information about F5 solutions for SDDC, visit f5.com/vmware and devcentral.f5.com/vmware.

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

Americas	Asia-Pacific	Europe/Middle-East/Africa	Japan
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com

Solutions for an application world.

VMware, Inc. 3401 Hillview Avenue, Palo Alto, CA 94304 877-486-9273 vmware.com