VMware Horizon View Optimized Secure Access

The F5 BIG-IP platform optimizes the VMware View user experience and ensures maximum performance, availability, scalability, and security.

White Paper

by Simon Hamilton-Wilkes
Principal Solution Engineer
VMware Alliance

Contents

Introduction

Desktop and endpoint device management has long been a challenge for IT organizations. Users demand flexibility, multiple access options, and desktop customization, while business units often require multiple desktop types based on business and technical requirements, with different RAM, display, and software configurations for each. This kind of multi-level matrix can be a major management headache on its own. Add in support for all the different desktop needs, plus remote support for those on laptops, and desktop management can all but consume an IT organization's budget and time.

VMware User Computing

VMware Horizon View—part of VMware's Horizon Suite of products—alleviates two major management headaches: location and standardization. To solve the location problem, virtual desktop infrastructure (VDI) deployments virtualize user desktops by delivering them to individual clients over the network from a central location. Those desktops are stored and run in the data center, rather than having individual desktop and laptop machines in the field running localized operating systems. This seamless virtualization goes undetected by users.

To solve the standardization problem, VMware enables business groups with specific desktop needs to be clustered together in the data center and managed as a unit. For example, when all the Windows machines need a new service pack, it can be installed to the master image in the data center, which is delivered to users the next morning when they log in. Because IT staff no longer have to visit each local system or push software installations down through remote tools, users aren't forced to reboot during the business day.

In addition to these location and standardization concerns, the user experience is consistently cited by organizations as critical to the success of virtual desktop deployments. Performance has to compare favorably to a conventional desktop while availability and security need to be even greater.

F5 offers a variety of solutions to help organizations maximize the success of these critical elements in their View desktop deployments. Together F5 and VMware have thoroughly tested and documented the benefits of using F5 Application Delivery Networking (ADN) solutions with VMware View to address needs for secure access, a single namespace, load balancing, server health monitoring, and more. To ensure that the core offering is compelling, F5 has released optimized packages to cost-effectively support secure remote access to View deployments of various sizes. These packages include the basic functionality and a streamlined configuration option to make their use simple and straightforward.

Performance, Scalability, and Security

The larger the VMware Horizon View deployment, the more View Connection Servers are needed to handle the concurrent desktop connections. VMware Horizon View Optimized Secure Access & Traffic Management by F5 provides valuable load balancing and health monitoring, resulting in higher system availability and greater scalability—and ultimately, a better user experience. Additionally, an F5® iApps® Template makes configuration straightforward, simplifying setup by providing the recommended settings and helping to prevent human error.

VMware View client connectivity utilizes multiple ports and protocols that must be directed at the same View Connection Server for a successful session. While PC over IP (PCoIP), the View desktop streaming protocol is UDP-based, but SSL-encrypted TCP connections are utilized for authentication and USB tunneling. Administrators can save capacity on the View Connection Servers by offloading this encryption to an F5 BIG-IP® ADC.

Enhancing Security and Access Control

Ensuring secure remote access is critical to protecting corporate information and often required in certain regulatory situations. To route incoming Horizon View connections to the internal network, a PCoIP proxy is needed in an organization's DMZ.

BIG-IP® Access Policy Manager® (APM) fulfills this function in a secure and scalable way. Placing BIG-IP APM in the DMZ avoids the need to expose sensitive Windows servers, Active Directory domain-joined servers, or View Connection Servers to the DMZ. It also eliminates the requirement for VMware Security Gateway servers in the DMZ. The BIG-IP APM appliance proxies the PCoIP connection, passing it internally to any available Connection Server within the View pod, which then interprets the connection as a normal internal PCoIP session. This provides the scalability benefits of a BIG-IP appliance and gives BIG-IP APM and BIG-IP® Local Traffic Manager™ (LTM) visibility into the PCoIP traffic, enabling more advanced access management decisions.

F5 has recently created four new optimized products—micro, small, medium, and large—to deliver a faster return on investment (ROI), extend functionality beyond any competitive offering, and ensure the investment in BIG-IP APM is appropriate for the size of the deployment. A streamlined iApps Template is also included to ease deployment. This custom iApp presents fewer configuration options than the full iApp for View, which can be used instead if advanced functions are required. Either iApp yields a configuration that can be modified as needed to address specific business and technical requirements.

These new F5 product options were developed in conjunction with VMware, which recognizes the additional capabilities BIG-IP APM brings to View and the limitations of the Security Server as a PCoIP proxy. The enhanced joint solution is easy for customers to deploy and support. Further options, including additional advanced traffic management options, a single namespace, and username persistence, are available when BIG-IP LTM is added to APM. (See the Resources section at the end of this document for more information.)

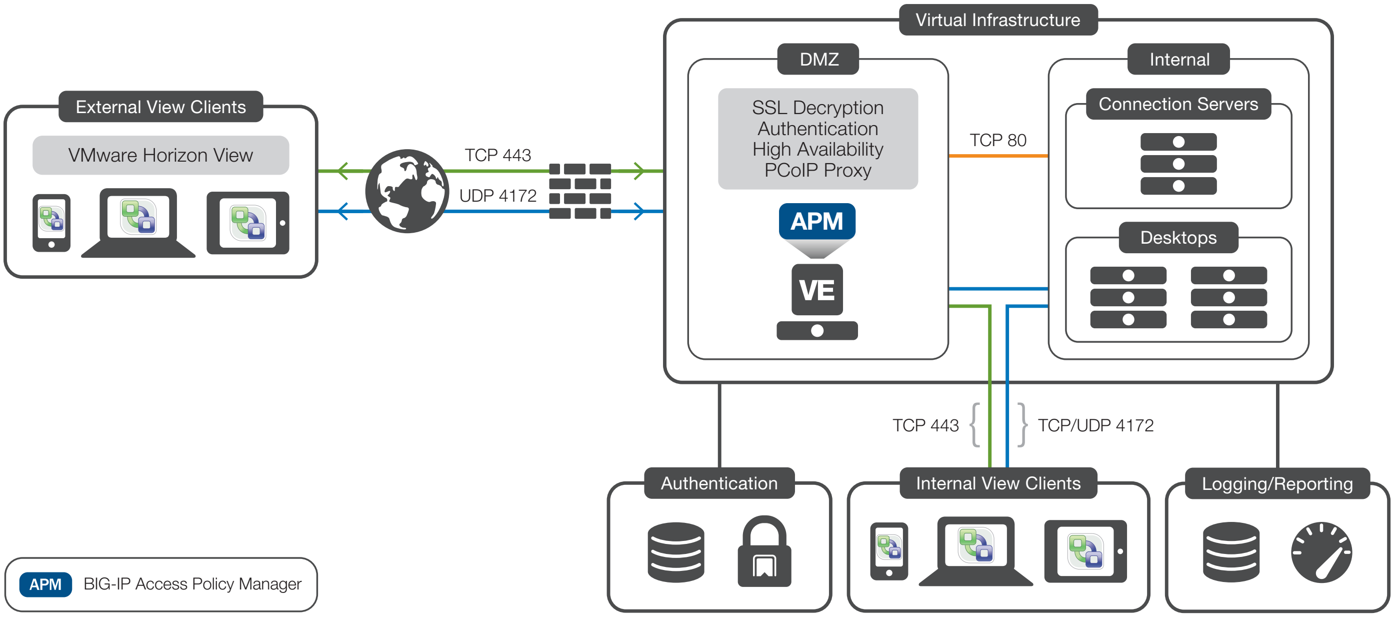

Figure 1: The F5 BIG-IP system and VMware Horizon View topology

Conclusion

There's no doubting the advantages of deploying a virtualized desktop solution like VMware Horizon View throughout the enterprise. By deploying the F5 BIG-IP system alongside it, organizations can achieve higher security, availability, and scalability while improving the user experience. With the straightforward deployment options delivered by proven iApps Templates and support for PCoIP proxy services, BIG-IP APM represents the best solution for secure remote access. In addition, new and optimized product offerings reduce both cost and deployment complexity to ensure a BIG-IP ADC becomes a standard View component. Furthermore, taking advantage of other BIG-IP modules—such as BIG-IP LTM and BIG-IP® Global Traffic Manager™ (GTM)—empowers IT staff to integrate multiple VMware View pods or physical sites for source desktops, all without disrupting users. By enabling users to reconnect to their existing persistent desktop source when required and providing a dynamic and agile infrastructure that can adapt to planned and unplanned events, the BIG-IP system becomes key to successful VMware View deployments.

Additional Resources

Deployment Guide for VMware View including Horizon View

Enable Single Namespace for VMware View Deployments

Username Persistence for VMware View Deployments

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

Solutions for an application world.