



What's inside:

- 2 Improving user experience
- 2 Enhancing security and access control
- 3 Application Performance and Availability
- 4 F5 and VMware View global configuration diagram
- 5 More Information

Integrating F5 Application Delivery Solutions with VMware View 4.5

VMware View™ is the leading desktop virtualization solution built for delivering desktops as a managed service—from the platform to the protocol. F5 optimizes end user experience, and helps ensure maximum performance, availability and security for VMware View implementations.

Organizations consistently cite the following criteria as critical for measuring the success of their virtual desktop deployments:

- End-user experience
- Performance and availability of desktops
- Security of the system
- Reduced desktop operating costs

F5 solutions help organizations maximize the success VMware View desktop projects. As a VMware partner, F5 has thoroughly tested and documented the benefits of using our application delivery networks with View 4.5 (as well as View 4.0). These solutions include secure access, single-sign-on, load balancing and server health monitoring.

Key benefits

Convenient Single Sign On

F5 enables authentication pass-through during the logon process. Log in once, and stay logged in as long as you are using the system.

Secure Access

F5 provides a broad range of authentication mechanisms, including two-factor schemes and various back-end directory services, as well as comprehensive pre-logon checks.

High Performance PCoIP

F5 devices enable all the security for transporting PCoIP communications but without the degradation in performance associated with many SSL VPN solutions.

Reduce bandwidth usage

F5 allows organizations to reduce bandwidth requirements while maintaining and even improving the end-user experience.

High Availability and Scalability

F5 provides valuable load balancing, health monitoring and SSL offload for VMware Connection Brokers resulting in higher system availability, and greater scalability of the existing server infrastructure.

F5 devices can apply quality-of-service functions so that PCoIP traffic receives priority over other traffic on the network. This ensures that no matter how busy the network may be, the virtual desktop user experience remains a positive one.

Benefits and F5 value

F5's application ready solution for VMware View ensures a secure, fast and available deployment, providing the following benefits to organizations, and their end users.

Improving user experience

F5's Application Ready Solution for VMware View helps provide the highest level of availability, performance, and end user satisfaction for VMware View deployments.

VMware View includes the high-performance PCoIP (PC over IP) communications protocol. Unfortunately, most traditional SSL VPN devices are unable to properly handle this unique protocol, and thus slow it down, thereby degrading the user experience.

F5 overcomes this issue with our Datagram Transport Layer Security (DTLS) feature. This transport protocol is uniquely capable of providing all the desired security for transporting PCoIP communications but without the degradation in performance. In addition, F5 supports View's automatic fallback to TCP if a high performance UDP tunnel cannot be established.

F5 devices can apply quality-of-service functions so that PCoIP traffic receives priority over other traffic on the network. This ensures that no matter how busy the network may be, the virtual desktop user experience remains a positive one.

One of the strengths of the F5's Application Ready Solution is the wide variety of functionality and documentation that ease the burden of configuring and optimizing our devices, freeing valuable IT resources to work on other projects. As part of the Application Ready Solution for VMware View, F5 has configured, tested and tuned our devices for VMware View. We have also carefully documented the procedures in our Deployment Guide, enabling an administrator to quickly, easily and accurately configure F5 devices for VMware View.

Enhancing security and access control

Secure access is a critical component of protecting corporate information. F5 addresses this need with pre-logout checks to the endpoint device prior to allowing the logon sequence to begin. F5 can determine if an antivirus or personal firewall is running on the PC and if they are up-to-date, or enforce a specific operating system patch level, among a host of other pre-logout checks. F5 can direct the user to a remediation page for further instructions or even turn on antivirus or firewalls for the user.

F5 also supports a broad range of authentication mechanisms, including two-factor schemes and various back-end directory services. F5 devices enforce Active Directory group policies on both corporate-owned and non-corporate-owned assets during the duration of the connection. Finally, once authenticated, F5 guarantees the encryption of all VMware View transport protocols, whether natively encrypted or not, without compromising performance. Using these features, the Edge Gateway is able to replace View Security Server.

Simplifying the authentication process for end users

Streamlining the authentication process for remote workers is important to the user experience. Users should be able to logon once and access their desktops immediately. Further, users should not have to manually re-logout every time their network connection gets temporarily interrupted. Fortunately F5 caches sign on credentials and enables authentication pass-through during the logon process. Log in once, and stay logged in as long as you are using the system. If your connection drops, it re-authenticates you automatically. This not only makes for a seamless user experience, but it minimizes the security risk and reduces password lockout calls to the help desk.

F5 technology, our devices are able to direct traffic with greater precision, resulting in a more uniform load distribution on the Connection servers.

Attacks do not always come from the outside of the network; internal users can gain sensitive information or sabotage applications with greater ease than external users. Because F5 devices can offload SSL encryption duties, organizations can encrypt traffic for entire transactions, without affecting performance for the end user. This allows organizations to use SSL 'everywhere' and prevents information from being sent in clear text over the internal network, mitigating risks associated with internal users as well as complying with state and federal regulations related to privacy. This also provides organizations a single location for certificate management, simplifying administration.

Application Performance and Availability

The larger the View deployment, the more View Manager Connection Broker servers needed to handle the concurrent desktop connections. F5 devices provide valuable load balancing, health monitoring and server resource offload functions (such as SSL processing) for the VMware Connection Brokers, resulting in higher system availability and greater scalability of the existing server infrastructure. This translates to a better user experience, lower server costs and reduced monthly operating expenses (such as power, space).

One of the unique features of F5's Application Ready Solution for View is the ability to persist client-to-broker connections on a session by session basis. Other implementations commonly use simple/source address persistence, where all the connections from a single IP address are sent to one server. Using F5 technology, our devices are able to direct traffic with greater precision, resulting in a more uniform load distribution on the Connection servers. In this way, F5 session persistence ensures that dropped connections are reconnected back to their existing desktop for fast re-access, with no need for re-authentication.

Monitoring device and application health

To further reduce the burden on the servers and increase productivity, F5 ensures applications are always available with advanced monitoring capabilities that help reduce the volume of traffic on the network and the burden on servers imposed by using valuable resources to respond to health checks. By passively monitoring application exchanges (such as data flows) through F5 devices to determine status, capacity, and data pertinent to load balancing decisions on performance and availability, F5 improves server efficiency, capacity, performance, and helps IT departments become a little more "green".

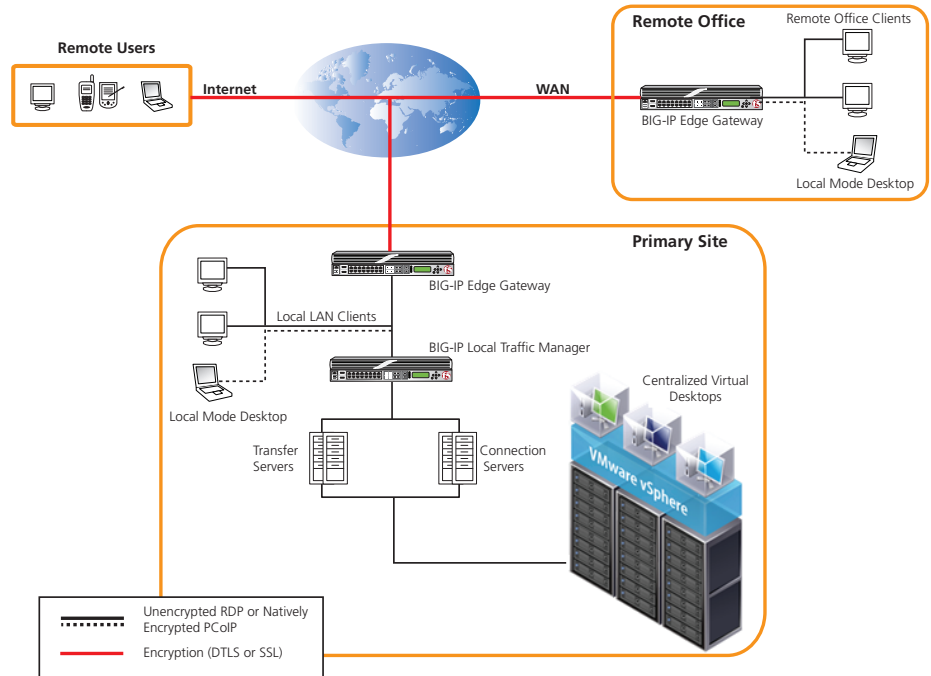
For patch management or maintenance windows, administrators can easily remove groups of devices from the F5 load balancing pool, perform patching or other maintenance while other devices remain in service. Once the maintenance is complete, those servers go back in the pool, and the remaining servers are taken down for maintenance, all with zero downtime.

F5 provides advanced tools that make it easy to manage our devices while maintaining flexibility and control of your infrastructure. F5 devices include a graphical reporting engine to display real-time historical statistics by the hour, day, week, or month. The dashboard reports statistics on CPU and memory usage, connections, and throughput with an easy-to-read graphical view. We make security compliance easy and save valuable IT time by enabling the exporting of policies for use by offsite auditors. Auditors working remotely can view, select, review, and test policies, without requiring critical time and support from the web application security administrator.

F5's Application Ready Solution for VMware View: Explore it. Deploy it. And run your business with it.

F5 and VMware View global configuration diagram

The following diagram shows a logical configuration example of the F5 solution for VMware View 4.5 using the BIG-IP Local Traffic Manager (LTM) and BIG-IP Edge Gateway. For more information on these products, see <http://www.f5.com/products/big-ip/>.



More Information

To learn more about F5 and VMware View, use the search function on F5.com to find these and other resources.

[F5 Solution Page](#)

[VMware](#)

[Deployment Guides](#)

[VMware View](#)

[VMware on DevCentral](#)

[VMware User Group](#)

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
info.asia@f5.com

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

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

