



APPLICATION READY NETWORK GUIDE MICROSOFT OFFICE SHAREPOINT SERVER 2007

Comprehensive Microsoft-Ready infrastructure that enhances the security, availability and performance of SharePoint 2007 deployments



SUMMARY

Hundreds of organizations around the world use Microsoft® SharePoint® with over 80 million implementations, allowing them to develop intelligent portals that seamlessly connect users, teams, and knowledge. With the release of Microsoft Office SharePoint Server 2007, F5 has specifically developed and tested a comprehensive Application Ready infrastructure that enhances the security, availability and performance of SharePoint deployments, whether it's over the LAN or across a global WAN.

Not only are organizations adding new and more robust, dynamic applications like SharePoint Server 2007 to their IT infrastructure, but the focus is starting to shift from simply adding boxes and installing a new application to the network, to looking at the network as a whole, and optimizing the entire infrastructure. As network-wide optimization becomes a priority, organizations are using tools like the Microsoft Infrastructure Optimization model¹ to help guide their strategy from a basic IT infrastructure that is overly complex, costly and difficult to manage, to a more dynamic infrastructure where costs are controlled, processes are fully automated, and integration and collaboration between users and applications is pervasive. F5 has a complete suite of application infrastructure technologies that can help simplify infrastructure and management, reduce costs and increase ROI, and improve security for SharePoint Server 2007 deployments, as well as the entire network and other applications. In essence, F5 has designed an integrated and adaptable application-ready network.

¹See [Microsoft Infrastructure Optimization model](#)

Benefits and F5 value

User Experience and Application Performance

One of the most important things to consider when deploying a centralized application like Microsoft SharePoint (and the one most often left to post deployment troubleshooting) is end user experience; will the application provide the necessary functionality in a timely manner? If an application is performing poorly because of configuration or infrastructure problems, end users will often abandon the application and official online processes and resort back to manual workarounds. Conversely, improving the performance of the application often leads to an increase in application adoption and user productivity.

F5 ensures the successful implementation of SharePoint by providing technology that guarantees the most efficient network possible. Because F5's unique TMOS operating system is a full proxy, it can optimize any end point that connects through the system. As a full broker of communications, the system optimizes every single end device communicating through it. This optimization can take place up and down the entire stack, from the transport layer to the protocol and application layer; functions outside the control of SharePoint. This takes the workload off of the servers for increased server efficiency. By reducing unnecessary protocol communication across the network, F5 improves application response times and utilization for SharePoint and other applications on the network.

F5 devices efficiently control the traffic flows for SharePoint deployments by optimizing client side delivery while maintaining server-optimized connections on the inside of the network.

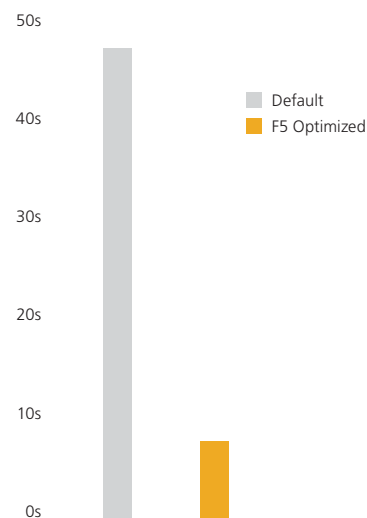
For example, when remote users connect to SharePoint Portal servers at varying connection rates, F5 independently handles each connection, optimizing end-user experience and server performance. F5 devices can also offload SSL and compression processing from the servers, freeing server resources and increasing server capacity for SharePoint 2007 deployments by more than 25%.

For users in remote offices, F5 has been shown to improve SharePoint application performance over high latency links on the order of 5 times, while reducing bandwidth by 30 times. F5's TCP optimizations also dramatically improve the reliability of WAN communications. Dial-up users connecting to Microsoft SharePoint Portal Server experienced connection reliability improvements of more than 40% while timeout errors were reduced by greater than 80%. These optimizations are particularly effective when delivering services over congested links.

And F5 has also worked to make the configuration of acceleration technologies simpler with the addition of application-specific policies. Simply choose the custom-built policy for Microsoft SharePoint from a list for out-of-the-box acceleration. F5 is the only vendor to bring practical and economic simplicity to support acceleration for both private (symmetric) and public (asymmetric users) under one management network.

When applications are responsive, especially core applications like SharePoint, adoption rates increase and users are more satisfied and productive. This leads to the added benefit of reducing the load on call centers and helpdesks, as users are less likely to call the IT department complaining about speed issues that usually have nothing to do with the application itself. This protects the investment in the application, minimizing the initial negative impact on the ROI of a new application deployment due to lost productivity and increased call volume.

Office SharePoint 2007
(in seconds)



F5 Optimizations provide a 5x increase in application performance over high latency links

Benefits and F5 value

Business Continuity and Disaster Recovery

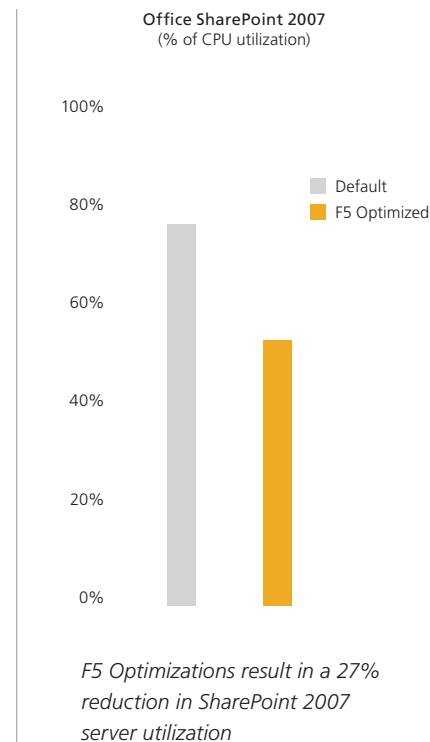
Because every minute an application is down or not responding properly can cost an organization thousands of dollars, deploying F5 devices with Microsoft Office SharePoint Server 2007 is essential for providing organizations with business-critical availability. Whether planning for a natural disaster, a pandemic like avian flu, trying to achieve regulatory compliance, or just carefully planning a new application deployment, F5 can help. F5 is the only vendor to virtualize data centers, VPN access, optimization and traffic in an integrated fashion.

F5 provides the industry's most comprehensive solution for site failover and business continuity. In addition to performing comprehensive site application availability checks, you can define the conditions for dynamically and transparently shifting all traffic to a backup data center, failing over an entire site, or controlling only the affected applications.

In a situation where employees cannot reach the office to work, but the data center is still

functioning, F5's SSL VPN provides secure remote access to the network and applications like Microsoft SharePoint that is much easier to use and scale than IPSEC – and much quicker to deploy and maintain in a disaster situation.

For organizations with multiple ISP links, F5 simplifies multi-homed deployments so you no longer need ISP cooperation, large bandwidth connections, designated IP address blocks, ASNs, or high-end routers to protect your network from ISP failures. Using DNS-based technology that removes the dependency on BGP to provide failover capabilities, the F5 eliminates multi-homed problems such as latency, high update overhead, and inferior traffic management, ensuring that users can always get to the SharePoint application. Organizations can benefit from guaranteed availability without delays or costly misrouting. It also gives you the ability to aggregate inexpensive links, with more granular control over which link to use based on performance, costs, and business policies.



Key Benefits

- F5 WAN optimizations increase SharePoint Portal Server performance by 5x
- Achieve 20 to 30 times bandwidth reduction for remote office SharePoint users
- Gain more than 25% server capacity with SSL and Compression offload
- Reduce timeout errors for dialup users by 85%
- Reduce deployment cycles by 1/3rd
- Automate failover, disaster recovery, and access control

Application Security

Most organizations have a solid security infrastructure in place for their network. Firewalls and other devices do an adequate job of protecting the network from attack. But these devices were not designed to protect against attacks targeting applications. Over 50% of all new vulnerabilities being identified on a weekly basis are attributed to web applications (SANS @RISK, "The Consensus Security Vulnerability Alert"). Protecting applications becomes even more important in today's global, partnership-driven economy, where partners and consultants are often given at least partial access to applications on the internal network.

Because SharePoint deployments often contain critical, sensitive internal information, making sure that the application is secure is not only important, it can be vital to the success of the business. Failure to keep data secure can be extremely costly, not only because of the value of the data itself, but the stiff penalties imposed for failing to meet compliance initiatives such as PCI, HIPAA, SOX, BASEL II, and other regulations.

Most of today's Intrusion Detection and Protection Systems, and even many application firewalls, are limited to guarding against a limited list of known attacks. But with the influx of new attacks targeting applications, this type of negative security protection isn't nearly enough. Unlike signature inspection methods, F5 also provides a positive security model, permitting only valid and authorized application transactions, while automatically protecting critical web applications from entire classes of HTTP and HTTPS-based threats (both known and unknown) such as Google hacking, cross-site scripting, and parameter tampering. F5, through our unique TMOS architecture and the power of iRules, enables full bidirectional session and payload inspection to ensure valid interaction with the application across multiple protocols.

F5 allows organizations to centralize application security, eliminating the need for multiple, redundant application security devices, greatly reducing the time and cost needed to deploy and

Benefits and F5 value

manage new applications like SharePoint 2007. We ensure your SharePoint application, and the information it contains, remains secure.

F5's comprehensive Endpoint Security for remote access gives your SharePoint deployment the best possible protection for (and from) remote users. F5 technology prevents infected PCs, hosts, or users from connecting to your network and the applications inside, and delivers a Secure Virtual Workspace, pre-login endpoint integrity checks, and endpoint trust management. F5 also enhances SharePoint application security and prevents application-layer attacks (e.g. cross-site scripting, invalid characters, SQL injection, buffer overflow) by scanning web application access for application layer attacks – then blocking user access when an attack is detected.

F5 products allow organizations to implement comprehensive application security, providing a centralized point of enforcement, and a coordinated and unified line of defense that lowers TCO and improves ROI.

Unified Security Enforcement and Access Control

In today's global economy, as organizations expand into new markets and grow through mergers and acquisitions, more and more organizations outsourcing development, services or applications, and are trying to cope with the need to extend the reach of their internal applications to partners, contractors and suppliers. This means that companies are faced with more users and devices attempting to access protected resources. Access control and enforcement is especially critical for SharePoint, as it is a collaboration tool and repository for shared documents. F5 provides a complete approach to providing access control regardless of end user, client type, application, access network or network resources.

F5 allows administrators to grant certain users – for example, business partners using equipment not maintained by the company – access to SharePoint and other extranet applications and sites. The F5 solution also includes centralized control for any access network and any device, with no need to deploy multiple access control solutions for remote users, wireless LANs, and the LAN.

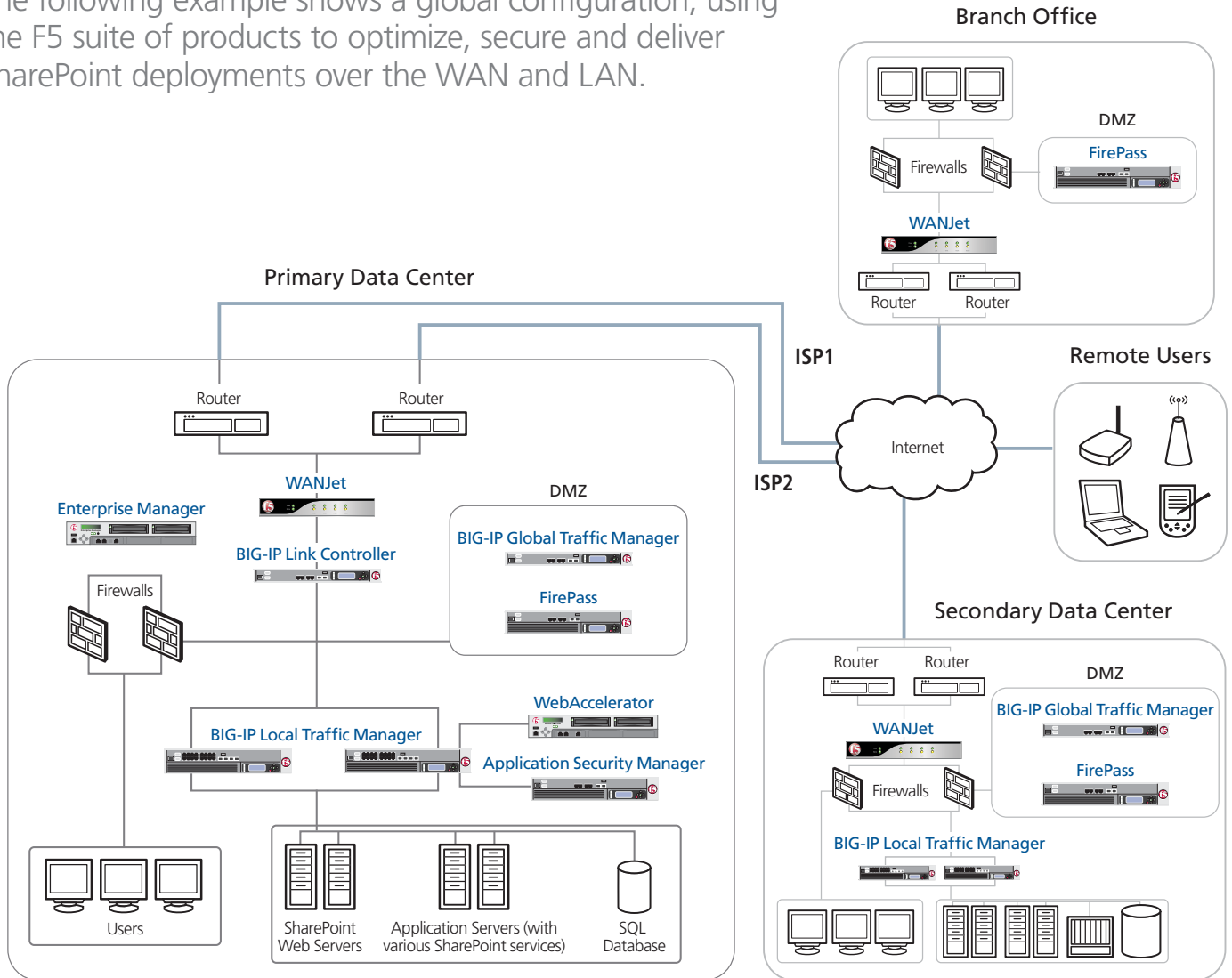
F5 simplifies policy and group management for IT departments, and provides central reporting and auditing, which reduces the overall cost of management. F5 has the most comprehensive end point security, enforcement, and auto-remediation, with no 3rd party software required.

One important aspect of F5's universal access approach is the ability to partition the network into various segments to protect and monitor access from one segment to the other. At the network level, you can use IP addresses, VLANs, MAC addresses, and packet filtering mechanisms to define practically any combination of network security policy based on any network parameter such as originating or destination VLANs, IP addresses, and protocols. You can refine this security with stricter access rules based on authentication results or application responses. With F5's iRules and the Universal Inspection Engine, you can define custom security policies. All of these capabilities can be used to implement LAN segmentation, different zones, such as trusted, public, private, protected, and so on.

The following example shows a global configuration, using the F5 suite of products to optimize, secure and deliver SharePoint deployments over the WAN and LAN.

Global F5 and Microsoft SharePoint Deployment

The following example shows a global configuration, using the F5 suite of products to optimize, secure and deliver SharePoint deployments over the WAN and LAN.



Additional Information

Microsoft SharePoint and F5 Solution Documents

Microsoft Office SharePoint Server 2007

[Deploying F5 with Microsoft Office SharePoint Server 2007](#). Includes the configuration for the BIG-IP LTM system, WebAccelerator module, and FirePass controller

HP White Paper:

[Deploying F5 Networks BIG-IP Local Traffic Manager with WebAccelerator for Microsoft SharePoint Server 2007](#)

Microsoft SharePoint Server 2003

- [Deploying Microsoft SharePoint Portal Server 2003 and the F5 BIG-IP System](#)
- [Deploying Microsoft SharePoint Portal Server 2003 and FirePass Controller](#)
- [Deploying Microsoft SharePoint Portal Server 2003 with the F5 WebAccelerator](#)

For more information about the partnership between F5 and Microsoft, see the [Microsoft Partner Showcase](#) on the F5 Solution Center.

F5 Product offerings

BIG-IP LTM

The BIG-IP LTM allows organizations to ensure quality of service and manageability, apply business policies and rules to content delivery, support increasing traffic volumes, deliver their applications securely, enjoy operational efficiency and cost control, and remain flexible to future application and infrastructure changes to protect their investments.

Product Modules (These modules can also be run as standalone appliances)

GTM: The BIG-IP Global Traffic Manager (GTM) Module provides high availability, maximum performance and global management for applications running across multiple and globally dispersed data centers. Seamlessly virtualizes FirePass VPN to automatically provide always-on access control.

ASM: The Application Security Module provides application layer protection from both targeted and generalized application attacks to ensure that applications are always available and performing optimally.

WA: F5 WebAccelerator™ is an advanced web application delivery solution that provides a series of intelligent technologies designed to overcome problems with browsers, web application platforms and WAN latency issues which impact user performance.

LC: The BIG-IP Link Controller Module seamlessly monitors availability and performance of multiple WAN connections to intelligently manage bi-directional traffic flows to a site – providing fault tolerant, optimized Internet access.

Feature Modules: These are individual feature packs that can be added to a BIG-IP traffic management platform. The Feature Modules include the Message Security, Intelligent Compression, L7 Rate Shaping, IPv6 Gateway, Advanced Client Authentication, SSL Acceleration, Fast Cache, and Advanced Routing Modules.

FirePass

F5's FirePass® SSL VPN appliance provides secure access to corporate applications and data using a standard web browser. Delivering outstanding performance, scalability, ease-of-use, and end-point security, FirePass helps increase the productivity of those working from home or on the road while keeping corporate data secure. Supports XP, Vista and Windows Mobile 5 clients, accessory Microsoft applications, including SharePoint, and integrates seamlessly with Active Directory.

WANJet

WANJet® is an appliance-based solution that delivers LAN-like application performance over the WAN. WANJet accelerates applications including: file transfer, e-mail, client-server applications, data replication, and others, resulting in predictable, fast performance for all WAN users.

Enterprise Manager

F5's appliance-based Enterprise Manager gives you the power to centrally discover and maintain the F5 devices in your network. With Enterprise Manager, you can archive and safeguard device configurations for contingency planning, Configure new devices from a central location without manually working on each device, easily and quickly roll-out software upgrades and security patches and much more.

iControl API

iControl is F5's SOAP API exposed on each BIG-IP LTM system. iControl supports Visual Studio and ASP to enable further automation between the application and the network. F5's developer community, DevCentral, has sample iControl applications and code. Visit the Microsoft page on [DevCentral](#) for [Microsoft-specific](#) forums and other useful information about F5 integration with Microsoft Applications.

F5 Acopia ARX

F5 Acopia award-winning intelligent file virtualization solutions decouple file access from physical file location. Our ARX products integrate seamlessly into existing Network Attached Storage (NAS), Windows®, UNIX® and Linux environments. ARX devices provide industry-leading scalability, performance and reliability, and are specifically designed to meet the needs of enterprise storage environments.



www.f5.com