



# APPLICATION READY NETWORK GUIDE MICROSOFT EXCHANGE SERVER 2007

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

Microsoft®  
Exchange Server 2007

## SUMMARY

Microsoft® Exchange® Server is the undisputed industry leader in corporate messaging. With the release of Microsoft Exchange Server 2007, not only does Exchange continue to provide rich, efficient access to e-mail, calendars, attachments, contacts, and more, but Exchange Server 2007 adds some exciting infrastructure and performance improvements as well. F5's comprehensive Application Ready infrastructure for Exchange Server 2007 allows organizations to easily provide additional performance, security and availability, to ensure maximum ROI with the minimum amount of work.

Organizations are increasingly taking a holistic approach to IT infrastructure, using valuable resources such as the new Microsoft Infrastructure Optimization (IO) model<sup>1</sup> to aid in creating a strategic plan for developing their IT infrastructures and realizing the maximum value from their technology investments. F5 has all the tools to help organizations optimize their entire network and achieve a truly dynamic infrastructure for Microsoft Exchange Server 2007 and other applications. This is F5's application-ready network.

---

<sup>1</sup>See [Microsoft Infrastructure Optimization model](#)

## Benefits and F5 value

### User Experience and Application Performance

Organizations depend on email as a vital communication medium. It is estimated that 70% of business is conducted over email. Users have come to expect that email communication is nearly instantaneous, and rely on its availability. Microsoft Exchange Server 2007 is a comprehensive messaging system that enables effective communication with a host of new and exciting features. When deploying such as powerful and integral application, organizations often neglect the role that the surrounding network plays in delivering such a complex application to what is often a global user base. F5 helps to smooth potential networking and infrastructure issues, to make sure that end-users receive the performance and reliability they expect from Microsoft Exchange.

Because email is so vital to a successful business, a market has been emerged for those who want to exploit it. Approximately 80% of internet traffic comes from abusive email. Exchange Server 2007, with its built-in defenses against SPAM and phishing e-mail, goes a long way toward reducing this type of email that reaches users. And F5 helps reduce this burden on Exchange Servers by providing a first layer of defense in the fight against SPAM. F5 has the industry's first reputation-based, perimeter anti-spam solution that is integrated into the application delivery control network. F5 leverages reputation data from Secure Computing's TrustedSource™ multi-identity reputation engine. This allows F5 to extend security for message applications to the edge of the corporate network, eliminating up to 70 percent of unwanted email. This keeps illegitimate messages from clogging up bandwidth and frees up capacity on the Exchange 2007 Edge Transport Servers.

F5 products can also offload other resource-intensive tasks from the Exchange servers, allowing the application to focus solely on the tasks for which it was designed. For example, F5 can offload SSL processing, compression, and caching from the Exchange Servers,

allowing them to concentrate on formatting and delivering the dynamic parts of the application. For example, in the standard implementation of Outlook Web Access, clients must download 160 objects from the Client Access server when they first log on. With F5 deployed, only six of those first requests are delivered by the Client Access servers, allowing those servers to spend more processing power on the delivery of actual mail.

F5's TMOS™ helps optimize many of the functions that are outside the control of Microsoft Exchange Server. At its core, TMOS is a full proxy: it can optimize any end point that connects through the system. With TMOS, F5 efficiently isolates clients from the server-side flows and independently maintains optimal performance for each connecting device, translating communications between systems. This allows F5 to improve application response times and utilization for Microsoft Exchange and other applications on the network, by reducing unnecessary protocol communication across the network.

This is particularly useful for Outlook Web Access, where one user might connect using broadband, while another is on dial-up. By isolating the client connections from the server connections, communication speed is not limited by the client – F5 devices buffer the data and are able to communicate at the fastest speed of each connecting device. And F5's TMOS already has full support for the majority of the new TCP optimizations that have been included in Microsoft's Vista® operating system. This provides users with the most effective use of the network regardless of the quality of their connection to the office.

Sound complex? Nearly all of these optimizations take place by default on F5 devices, with no additional configuration necessary. And for specific applications like Microsoft Exchange 2007, F5 makes improving application performance as easy as selecting the custom built policy for Exchange 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

With F5, users with email attachments, such as Office 2003 Word documents or Excel files, experience a 90% reduction in download time.

private (symmetric) and public (asymmetric users) under one management network. Multiple F5 products contain custom built configuration sets specific to Microsoft Exchange Server or Outlook Web Access.

F5 has built intelligence into its products to recognize and handle email attachments in Outlook Web Access in the most efficient manner. This can provide significant improvements for home and mobile users. With F5, users accessing email attachments, such as Office 2003 Word documents or Excel files, experience a 90% reduction in download time. PDF document attachments are also linearized for faster rendering on the clients machine, allowing users to view the first pages of the PDF file as the rest of file loads. Additional steps are taken to flag attachments for optimal storage in the client's browser cache. All of these improvements are meant to streamline the impact of various network conditions to ensure a usable and high performing application.

An application that is performing optimally makes end users much more satisfied and productive. Organizations using Microsoft Exchange Server essentially rely on this application as a key to the success of the business. F5 helps protect the investment in the application, minimizing the initial negative impact on the ROI of a new application deployment due to issues outside of its control.

## Benefits and F5 value

### Business Continuity and Disaster Recovery

Even a perfect application in a highly optimized network doesn't help if users can't get to it. More and more organizations are putting comprehensive plans in place to make sure that business continues as usual in the case of disruptive events like natural disasters, pandemics like avian flu, or even new regulatory requirements. In today's global economy, business does not stop because of an outage or disaster in one region.

For Exchange 2007, F5 can provide reliable, real-time availability of globally dispersed Edge Transport servers. If one datacenter goes down, F5 immediately recognizes that it is unavailable, and seamlessly re-routes incoming email to the available datacenter. When the datacenter comes back up, F5 immediately starts sending connections back to both locations.

One of the exciting new features in Microsoft Exchange 2007 is Continuous Cluster Replication (CCR), which provides geographically-distributed high availability for mailbox servers. F5 can help ensure rapid replication to reduce or eliminate potential data loss in the event of a failure, improve end-user experience during the failover period, and greatly decrease time-to-recovery, all the while reducing bits-on-the-wire.

When a disaster or other problem does occur, F5 has a host of options for ensuring employees have secure remote access to Exchange 2007 and the corporate network. F5 allows you to easily create a custom application tunnel for accessing Outlook Web Access or Microsoft Outlook, so a user only has to click a link to securely access their mail. F5 can dynamically format email from Microsoft Exchange Servers to fit the smaller screens of mobile phones and PDAs.

For organizations with more than one ISP link and multiple sites, F5 simplifies inter-site message transfer, 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. F5 eliminates the dependency on BGP to provide failover capabilities ensuring that Exchange Server 2007 Hub Transport servers can route

messages between sites without administrator intervention even when ISP link goes down.

### Application Security

Providing security specific to an application deployment is fast becoming an essential component of launching a new application.

Organizations must ensure that security personnel work closely with the network and application teams to ensure the successful and secure deployment of an application, especially one like Microsoft Exchange, which is often used by all employees, everyday. F5 has a number of ways to help increase the security of Exchange 2007 deployments.

F5's message security offering provides an additional layer of protection to the Exchange 2007 deployment. SPAM email can contain virus attachments and other malicious content, like phishing attempts and Trojan attacks. By eliminating 70% of unwanted email before it even reaches the Exchange Servers, F5 greatly reduces the chance that an unwanted and potentially dangerous email gets through to the Exchange 2007 servers.

Exchange 2007 Continuous Cluster Replication allows Exchange information to be passed from the active server node to a geographically dispersed passive server node. To provide additional security for Continuous Cluster Replication, F5 ships the transaction log files between the active and passive server nodes in an encrypted tunnel, preventing clear text from being passed on the wire.

For remote users who might be trying to access Microsoft Office Outlook or Outlook Web Access from an airport kiosk or other unknown device, F5's comprehensive Endpoint Security provides the best possible protection for 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.

And when the remote user has finished their session with Outlook or Outlook Web Access, F5's post logon security protects against sensitive information being left on the client. F5 can impose a cache-cleaner to eliminate any user residue such as browser history, forms, cookies,

auto-complete information and more. Post logon security can also be configured to close Google® desktop search so nothing is indexed during the session. Post logon actions are especially important when allowing non-trusted machines access without wanting them to take any data with them after the session.

### Unified Security Enforcement and Access Control

Not only is security essential to an application deployment, but the act of enforcing security policies and controlling access to applications is equally important. F5 universal security enforcement and access control can work with Microsoft Exchange 2007 to ensure an extremely high level of protection for and from remote users, regardless of end user, client type, application, access network or network resources.

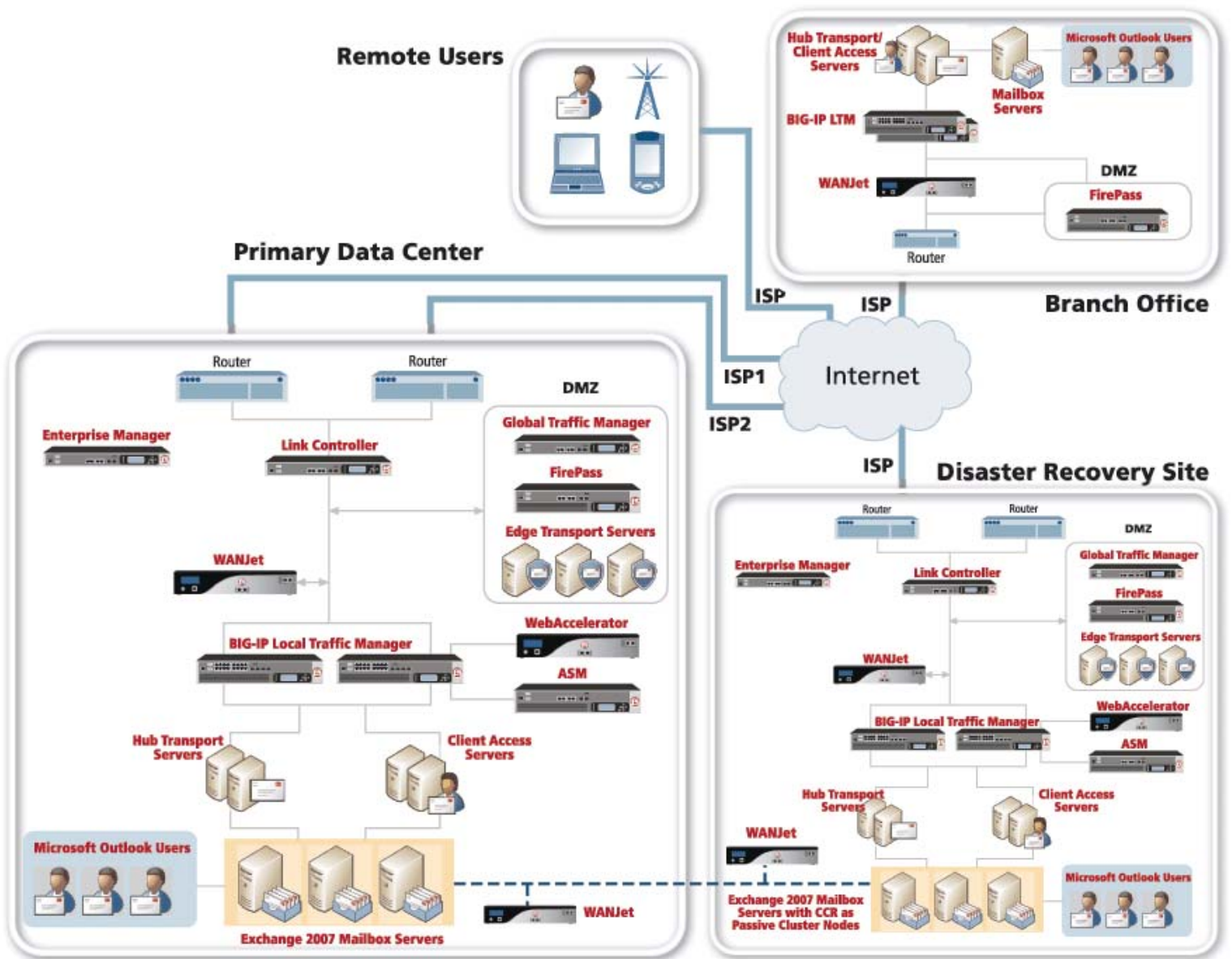
Most organizations don't necessarily want all users or devices to access to all resources all the time. F5 Pre-logon checks and Protected Configurations provide the ability to grant users full access to Exchange (after satisfying all security policy requirements) using Office Outlook; while users who meet only some of the criteria are restricted to Outlook Web Access only. For users who are authorized, but do not meet predefined device-based security requirements, F5 technology can create a secure area on the client PC, called the Protected Workspace, for that session and have the user enter their sensitive information with a Secure Virtual Keyboard.

F5 can also partition the network into various segments to protect and monitor access from one segment to another. You can use IP addresses, VLANs, MAC addresses, and packet filtering mechanisms to define nearly 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.

F5 simplifies policy and group management, and provides central reporting and auditing, which reduces the overall cost of management.

# Global F5 and Microsoft Exchange Server Deployment

The following example shows a global configuration, using the F5 suite of products to optimize, secure and deliver Exchange 2007 deployments over the WAN and LAN.



## Additional Information

### Microsoft Exchange Server and F5 Deployment Guides

F5 Deployment Guides give you detailed, step-by-step procedures on how to configure F5 devices with Microsoft Exchange Server and Outlook Web Access.

### Microsoft Exchange Server 2007

- [Deploying F5 and Microsoft Exchange Server 2007](#)

### Microsoft Exchange Server/ OWA 2003

- [Deploying Microsoft Outlook Web Access 2003 and the F5 BIG-IP LTM System](#)
- [Deploying Microsoft Exchange Server/ Outlook Web Access 2003 and FirePass Controller](#)

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 Local Traffic Manager (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 (an excellent addition to Exchange Server 2007), 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](http://www.f5.com)