



What's inside:

- 2 Improving application performance and user experience
- 3 Enhancing application security
- 4 Providing unified security enforcement and access control
- 5 Enabling seamless business continuity and disaster recovery

F5 enables a secure, agile, and optimized Microsoft Exchange Server 2010

Microsoft® Exchange® Server is still the undisputed industry leader in corporate messaging. The latest version, Microsoft Exchange Server 2010, helps users get more done by improving access to all of their communications—e-mail, voice mail, instant messaging—from virtually any platform, Web-browser, or device through industry standard protocols. F5 works closely with Microsoft in Redmond to ensure we are delivering the best possible technology and deployment guidance to support highly available and scalable Exchange 2010 deployments.

F5 has all the tools to help organizations optimize their entire network and achieve a truly dynamic infrastructure for Microsoft Exchange Server. From providing custom-built Exchange application templates to optimizing and securing Exchange 2010 traffic over the WAN, F5's comprehensive Application Ready solution for Exchange Server 2010 allows organizations to easily provide additional performance, security and availability, to ensure maximum ROI with the minimum amount of work. F5 enables IT agility, your way.

Key benefits

Secure and Fast Mailbox replication

F5 can perform Database Availability Group replication across data centers inside a encrypted tunnel for secure, optimized mailbox replication for the entire mailbox store

Gain Exchange Server capacity

Extend server capacity by offloading tasks like compression and SSL processing onto F5's unified, simple to manage platform.

Reduce download times for end users

F5 helps drastically reduce download time for email attachments.

Eliminate SPAM before it reaches the Exchange Servers

F5 technology can help eliminate more than 70% of unwanted email before it reaches your Exchange Servers.

Increase administrator efficiency

F5's Microsoft Exchange application templates and step-by-step configuration guidance help reduce deployment cycles by 1/3rd.

Secure your Exchange deployment

From powerful network- and protocol-level security to attack filtering, F5 protects Exchange deployments that help run your business.

F5 Increases Server Efficiency

F5 optimizations dramatically reduce the number of objects the Client Access Servers have to deliver to the clients, allowing those servers to spend more processing power on the delivery of actual mail.

Benefits and F5 value

F5's application ready solution for Microsoft Exchange Server 2010 ensures a secure, fast and available deployment, providing the following benefits to organizations, and their end users.

Improving application performance and user experience

Today's organizations depend on messaging applications, with an estimated 70% of business conducted over email. Users have come to expect that email communication is nearly instantaneous, and rely on its availability. Microsoft Exchange Server 2010 is the latest in a long line of industry-leading messaging systems from Microsoft that enables effective communication with a host of new and updated features. F5 helps ensure that IT departments, and their end-users, receive the performance, reliability and constant availability they expect from Microsoft Exchange Server.

One significant change in Microsoft Exchange Server 2010 is that all user access to E-mail, regardless of protocol, is done through Client Access Servers. This is important, because it allows F5 to intelligently direct *all* Exchange Server client traffic. For example, F5 provides built-in MAPI acceleration, which uses symmetric adaptive compression and symmetric data de-duplication to dramatically improve performance and reduce bandwidth usage for customers using Microsoft Exchange, especially when sending email attachments.

Another new feature in Microsoft Exchange Server 2010 is the addition of Database Availability Groups (DAG). A DAG is a group of up to 16 Mailbox servers that host a set of databases and provide automatic database-level recovery from failures that affect individual servers or databases. F5 optimization technology speeds mailbox database replication between DAG members while simultaneously reducing the total amount of data transferred over the WAN connection. F5 can also encrypt the optimized tunnel, securing the replication even when traversing untrusted or public networks.

With the workforce becoming increasingly mobile, Microsoft has done a great job in ensuring users can access their email from a wide range devices. But because these devices are connecting with the Exchange Server over the WAN, there are a number of different factors that can affect the performance of the Exchange Servers that have nothing to do with the application itself. IT managers often assume that adding bandwidth will solve the problem. But TCP throughput degrades significantly on the WAN, particularly on high-latency, long distance links, so adding bandwidth is often ineffective.

F5 helps smooth these potential networking and infrastructure issues, allowing Microsoft Exchange to focus solely on the tasks for which it was designed. F5's TCP/IP stack is standards-based and contains hundreds of improvements that affect both WAN and LAN efficiencies. For low-speed WANs, F5 detects client speed and estimates bandwidth to limit packet loss and recovery in the case of dropped packets. It improves transfer rates for all connecting client types and increases bandwidth efficiency across the WAN. F5 solutions dynamically and automatically optimize TCP window sizes and TCP congestion information for each connection symmetrically and asymmetrically (every client and every server), improving throughput in high loss networks. This provides users with the most effective use of the network regardless of the quality of their connection to the office.

For example, for Outlook Web App, F5 optimizations dramatically reduce the number of objects the Client Access Servers have to deliver to the clients, allowing those servers to spend more processing power on the delivery of actual mail. F5 has also built intelligence into our products to recognize and handle email attachments in Outlook Web App in the

F5 Helps Eliminate Spam

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 2010 servers.

most efficient manner. 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.

Because email is so vital to a successful business, there is also a market for those who want to exploit it. Approximately 80% of internet traffic comes from abusive email. This junk email is not only potentially harmful, but email systems have to spend valuable system resources processing these messages, putting unnecessary strain on the servers. Exchange Server 2010, with its built-in defenses against spam and phishing e-mail, goes a long way toward reducing the amount of this type of email that reaches users. F5 helps reduce the burden on Exchange Servers by stopping unwanted email before it even reaches the Exchange servers. F5 provides a reputation-based, perimeter anti-spam solution that is integrated into the application delivery control network. 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 2010 Edge Transport Servers.

Sound complex? Nearly all of these optimizations take place by default on F5 devices, with no additional configuration necessary. As part of our Application Ready Solution for Microsoft Exchange, we have configured, tested, and tuned our devices with Microsoft Exchange Server 2010, and carefully documented the procedures in our deployment guides, making it easy to reproduce this optimized configuration. And for the popular Outlook Web App and RPC Client Access components of Exchange 2010, this tested and optimized configuration is available as an application template. The template requires a minimum amount of information and only minutes of time from an administrator to quickly, accurately, and optimally configure F5 devices for Microsoft Exchange 2010. F5 has also created custom configuration profiles and policies for Exchange and Outlook Web App, with some acceleration and security policies including list items for Exchange/OWA make configuration extremely simple, yet powerful and flexible.

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.

Enhancing application security

Providing security specific to an application deployment is fast becoming an essential component of launching and maintaining a new application. Security personnel must 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 2010 deployments.

F5's message security offering provides an additional layer of protection for Exchange 2010 deployments. Spam email can contain virus attachments and other malicious content, like phishing attempts and Trojan attacks. The F5 solution leverages reputation data from the McAfee® TrustedSource™ multi-identity reputation engine to accurately filter email. 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 2010 servers.

And now, all data can be symmetrically encrypted between local and remote F5 devices, providing a new way to ensure site-to-site data security by preventing clear text from being passed on the wire. This secure connection, or tunnel, also improves transfer rates, reduces bandwidth, and offloads applications for more efficient WAN communication. As mentioned previously, F5 can perform DAG replication across data centers inside this encrypted tunnel for secure mailbox replication for the entire mailbox store.

For remote users who might be trying to access Microsoft Office Outlook or Outlook Web App 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 App, 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 desktop search applications 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.

F5 security devices report previously unknown threats (such as brute force attacks and zero-day web application attacks) and mitigate web application threats, shielding the organization from data breaches. Our full inspection and event-based policies deliver a greatly enhanced ability to search for, detect, and apply numerous rules to block known L7 attacks.

F5 makes security compliance easy and saves 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.

Not only does F5 provide comprehensive application security, but produce extremely secure devices. We help make sure your Microsoft Exchange Server deployment, and the information it contains, remains secure.

Providing 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 2010 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.

F5 provides centralized access and application availability services to users based on the context of the user and the application they are accessing. By driving application and user identity into the network, organizations have a more centralized, repeatable and cost effective way to scale up access control services. This new simplified access management system allows users to easily access approved web applications and networks without multiple authentications for greater worker productivity. <Dayne verifying this paragraph from an APM perspective and making more exchange specific>>

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 provides organizational efficiency and an easy way to scale management by partitioning our devices into administrative domains, allowing a single F5 device to be managed by multiple application teams without interference. For example, the application owner for the Microsoft Exchange can be given permission to only view or modify objects which reside in that particular domain. This increases productivity by reducing the time spent in meetings, tracking down appropriate administrative personnel, and improves the ability of application administrations to manage applications when it's necessary. F5 helps streamline the business process and improve the productivity and efficiency of operational personnel.

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

Enabling seamless business continuity and disaster recovery

Even a perfect application in a highly optimized and secure 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 the H1N1 flu, or even new regulatory requirements. In today's global economy, business does not stop because of an outage or disaster in one region.

User experience suffers when organizations with distributed data centers are unable to allocate global traffic by routing the user to the best and closest data center based on specific business policies. Changing network and user conditions can overwhelm a data center during peak traffic times. F5 provides comprehensive application management services that support evolving application requirements, enabling real-time load balancing across data centers.

For Exchange 2010, F5 can provide reliable, real-time availability of globally dispersed Edge Transport servers (SMTP). If one data center goes down, F5 immediately recognizes that it is unavailable, and seamlessly re-routes incoming email to the available data center. When the data center comes back up, F5 immediately starts sending connections back to both locations.

And F5 can help ensure secure, rapid replication of Exchange 2010 DAGs 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.

F5 improves business continuity with advanced monitoring capabilities that not only maintain availability, but can also 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, and performance.

Global Availability

F5 provides reliable, real-time availability of globally dispersed Edge Transport servers (SMTP). If one data center goes down, F5 immediately recognizes that it is unavailable, and seamlessly re-routes incoming email to the available data center

When a disaster or other problem does occur, F5 has a host of options for ensuring employees have secure remote access to Exchange 2010 and the corporate network. F5 allows you to easily create a custom application tunnel for accessing Outlook Web App or Microsoft Outlook, so a user only has to click a link to securely access their mail. F5 can dynamically format email from Exchange Servers to fit the smaller screens of mobile phones and PDAs. F5 enables context aware, policy controlled, secure access to applications providing LAN speed performance for remote users.

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 2010 Hub Transport servers can route messages between sites without administrator intervention even when ISP link goes down.

F5's Application Ready Solution for Microsoft Exchange Server 2010: Explore it. Deploy it. And run your business with it.

More Information

To learn more about F5 and Microsoft Exchange Server, use the search function on F5.com to find these and other resources.

Application Page

[Microsoft Exchange Server](#)

Deployment Guides

[Microsoft Exchange Server 2010](#)

[Microsoft Exchange Server 2007](#)

[Microsoft Exchange Outlook Web Access 2003](#)

Microsoft Solutions Page on DevCentral

<http://devcentral.f5.com/microsoft>

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

