F5 enables secure, agile, and optimized Exchange Server 2010 deployments

Microsoft® Exchange® Server is the undisputed industry leader in corporate messaging. Microsoft Exchange Server 2010 provides businesses with email, calendar, and contacts on the PC, phone and web, so employees can stay connected and in sync. F5 works closely with Microsoft 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 achieve a truly dynamic infrastructure for Microsoft Exchange Server. From providing custom-built Exchange iApp™ templates for simple, error-free deployments, to optimizing and securing Exchange 2010 traffic over the LAN and 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

Increase administrator efficiency and accelerate deployments
F5’s iApp templates for Exchange enable you to streamline design and implementation, resulting in a fast, accurate deployment or upgrade.

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

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

Reduce download times
F5 helps drastically reduce the download time of email attachments for end users.

Eliminate SPAM before it reaches the Exchange Servers
F5 can help eliminate more than 70% of unwanted email before it reaches your Exchange Servers, increasing Exchange Server efficiency

Exchange-specific analytics
Get real-time visibility into application and user performance specific to your Exchange deployment.
Why F5?

F5 Networks is the market share leader in Application Delivery Networking, focused on ensuring the secure, reliable, and fast delivery of applications like Exchange 2010. The following is an overview of why so many businesses rely on F5 to be the strategic point of control for their Microsoft Exchange Server 2010 investments.

F5 has a broad and deep partnership with Microsoft
- Microsoft and F5 have a global partnership that spans more than 11 years
- F5 is a MPSC Alliance partner with offices and a lab at the Microsoft headquarters in Redmond, Washington
- F5 is one of only 60 Microsoft Technology Center Alliances Program partners
- F5 works with Microsoft on solution development across products and technologies
- F5 provides training for Microsoft technical field, services and support teams

F5 adds more value with the changes in the architecture of Exchange
- All Exchange clients (regardless of protocol) connect via the Client Access Server role, increasing the importance of F5’s strategic location in the data center
- Microsoft requires load balancing for Client Access Servers, and recommends hardware-based load balancing; F5’s wide variety of platforms and solutions are a perfect match for Exchange deployments of any size
- The F5 solution is flexible, yet powerful enough to use for Exchange 2010 as well as the other Microsoft UCC applications, like SharePoint and Lync Server

F5 increases Exchange performance by offloading SSL and other services
- Offload SSL onto F5 devices to significantly increase the ability of Exchange to service incoming user connections
- Gain Exchange server capacity by performing compression and caching on F5 devices
- Conserve resources by eliminating up to 70% of SPAM before it reaches Exchange

F5 ensures your Exchange 2010 deployment remains secure
- Enhance Exchange 2010 security with intelligent application-layer protection
- Prevent unauthorized access and enforce anti-virus levels and other policies with pre-logon checks for web clients that ensure corporate compliance
- Keep corporate data secure with post-logon checks and clean-up controls that ensure sensitive data is not left on public computers or kiosks
- Set granular, easy-to-configure secure access policies that assign permission levels depending on the device being used (such as mobile device, kiosk, or work PC)

F5 helps keep end users, and Exchange administrators productive and satisfied
- Deploy in minutes while mitigating the risk of failed or delayed deployments with iApp templates for Exchange 2010
- Ensure users are always directed to fully-functional resources with sophisticated iApp-created health monitors which log in to individual Client Access Services
- Consolidate infrastructure and simplify web access with F5 cross-site load balancing and site resilience
- Gain a comprehensive view of users, the Microsoft Exchange application, and the network, which helps better respond to changing business needs
Detailed Benefits and F5 Value for Exchange Server 2010

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.

**F5 improves Exchange 2010 end user experience and application performance**

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. F5 solutions enable businesses to achieve strategic points of control for their Exchange deployments, helping ensure that IT departments, and their end-users, receive the performance, reliability, and constant availability they expect from Microsoft Exchange Server.

**Deploy quickly and accurately with built-in, Exchange-specific application services**

As part of F5’s Application Ready Solution, our engineers meticulously configured, tested, and fine-tuned our devices for Exchange 2010. F5 has worked closely with Microsoft during this process, regularly re-testing and updating the solution, as well as incorporating customer feedback, to make sure this solution improves while Exchange 2010 matures in the market.

As a result, F5 has created an Exchange-specific application template, called an iApp, which acts as the single point interface for building, managing, and monitoring Exchange 2010 across the entire F5 solution. This allows you to deploy and control functionality like single sign on, secure remote access, intelligent load balancing, and advanced health monitoring, on one device, as a single application service. An administrator spends a few minutes answering questions about the Exchange deployment, and the iApp creates an optimized F5 configuration, saving weeks or even months of development time.

Once your F5 deployment for Exchange is up and running, F5 provides real-time performance statistics, and diagnostic and troubleshooting information such as application response time, network latency, and connection statistics, which are specific to the Exchange application. With this application-centric view, there is no longer a need to try to extrapolate meaningful analysis from statistics for individual configuration objects.

**Optimize Exchange Server 2010**

One significant change in Microsoft Exchange Server 2010 is that all user access to email, regardless of protocol, is done through Client Access Servers. This is important because it allows F5 to intelligently direct all Exchange Server client traffic, even internal users. This enables F5 to apply optimizations—such as caching, compression, TCP connection optimization, and SSL offload—that increase availability, performance, and security for Exchange Server, making F5 a natural fit in an Exchange Server environment.
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.

F5 optimization technology speeds mailbox database replication between DAG members while simultaneously reducing the total amount of data transferred over the WAN connection.

Increase Exchange Server performance over the WAN

With the workforce becoming increasingly mobile, Microsoft has done a great job in ensuring users can access their email from a wide range devices. However, 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 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.

Reduce load on the servers while helping protect your Exchange deployment

Because email is so vital to a successful business, the market for those who want to exploit it is constantly growing. Approximately 80% of internet traffic comes from abusive email. 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 with an inexpensive, easy-to-use, reputation-based SPAM filtering solution that stops up to 70% of unwanted email on the edge of the corporate network, before it even reaches the Exchange servers. This significantly reduces the amount of mail the Exchange Server (or solution like ForeFront Endpoint Protection for Exchange) has to process. This highly customizable solution enables organizations to easily determine the mail that is simply dropped, sent along to the user, or sent to a more sophisticated scanning engine for further processing.

As an additional benefit, the F5 solution can also reduce archiving and retention costs that are required to keep in compliance with new regulations. By preventing 70% of the email from reaching the servers, there is now 70% less email to archive and store, a considerable savings.

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.

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.

F5 enhances application security for Exchange Server 2010
Providing security specific to an application deployment is 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, all day, every day. F5 has a number of ways to help proactively reduce threats, and increase the security of Exchange 2010 deployments.

Security for (and from) remote users
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. This solution includes a customizable
policy engine for defining Microsoft Exchange access, authentication, and authorization across users, devices and network locations. This helps organizations define and enforce a robust security posture for Exchange – including difficult to secure mobile devices.

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.

Secure data over the WAN
With F5, 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. And F5 can perform Exchange DAG replication across data centers inside this encrypted tunnel for secure mailbox replication for the entire mailbox store.

F5 message security increases protection
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.

Security from known and unknown attacks
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, best-in-class application security for protecting Exchange, but we have the only Application Delivery Controller certified as a network firewall. We help make sure your Microsoft Exchange Server deployment, and the information it contains, remains secure.

Providing unified security enforcement and access control for Exchange 2010

Security is 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 centralizes web single sign on and access control services, and 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. With F5, you can converge and consolidate remote access, LAN access, and wireless connections within a single management interface, and providing easy-to-manage access policies, helping you free up valuable IT resources and scale cost-effectively.

Simplify access management

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, such as Outlook Web App, and networks without multiple authentications for greater worker productivity.

Many solutions use application coding, web server agents, or specialized proxies or servers to manage application access. With AAA control directly on the F5 device, you can apply repeatable access policies across many applications and servers while gaining centralized visibility of your authorization infrastructure. F5 enables you to consolidate infrastructure, eliminate redundant tiers, simplify management, and significantly reduce capital and operating expenses.

Granular access control

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 Microsoft Office Outlook; while users who meet only some of the criteria are restricted to Outlook Web App 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 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 for Exchange 2010

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, or even new regulatory requirements. In today’s global economy, business does not stop because of an outage or disaster in one region.

Real-time global traffic management for Exchange

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.

F5 enables high availability for Client Access Server arrays, both in the local data center and also across multiple data centers. Because Exchange is deployed with Client Access and HUB arrays near every deployment of mailbox servers, F5 can ensure traffic is intelligently directed between clients and the best Client Access Server array. This includes geolocation (finding the best Client Access Server array based on user location with respect to available arrays) and site resilience (real-time knowledge of the health of each Client Access Server array and when to failover to a back up array).

F5 can also 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.

Simplify data center fail-over for maintenance windows

With F5, directing application traffic to a specific data center does not always have to be a result of a disaster or outage, it can be part of the regular maintenance plan. You can effortlessly and transparently direct traffic for a specific application like Exchange, or all traffic, to a specific data center for maintenance windows, even those that occur during normal business hours. In the event a disruptive event does happen, no one panics as the technology and IT operations process are in place and well-rehearsed.

Sophisticated monitoring keeps users connected to Exchange

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 non-disruptively 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.
As a result of our extensive testing with Exchange 2010, we found that simply monitoring the UP/DOWN status of the Exchange servers is not always a sufficient way to check the health of servers. The iApp template now includes the ability to create advanced monitors that actually log in to most Exchange Client Access services and check for valid content in the response. This ensures the Exchange services are not only available, but functioning properly.

Secure, remote access ensures business continuity
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 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 Border Gateway Protocol (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.
F5 Global Configuration Diagram for Microsoft Exchange Server 2010

The following logical diagram shows a global configuration using the F5 suite of products to optimize, secure, and deliver Microsoft Exchange Server 2010 deployments over the WAN and LAN.
More Information

To learn more about F5’s Application Ready Solution for Microsoft Exchange Server 2010, use the search function on F5.com to find these and other resources.

Application Page
Microsoft Exchange Server 2010

Deployment Guides
Microsoft Exchange Server 2010 for BIG-IP v11.x
Microsoft Exchange Server 2010 for BIG-IP v10.x
Microsoft Exchange Server 2007

White Papers
Hardware Load Balancing for Optimal Microsoft Exchange Server 2010 Performance
Secure, Optimized Global Access to Corporate Resources

Case Studies
A.T. Kearney
Human Rights Watch
Sysmex America
Reliance Protection

Microsoft Solutions Page on DevCentral
http://devcentral.f5.com/microsoft

F5 Product Offerings
BIG-IP Product Family (Application Delivery Controller)
FirePass (SSL VPN)
Enterprise Manager (F5 Device Management)
ARX Series (File Virtualization)
Data Manager (File Virtualization)