Architect Your Network for a Successful Exchange 2013 Deployment

Microsoft Exchange 2013 offers new ways for your organization to support user productivity, meet security challenges, and maintain control over confidential data. Business email, calendars, and contacts are available to users on almost any device, and new collaboration features provide tools to help people work together more effectively. Built-in email attack defenses and data loss prevention features that protect users from mistakenly sending sensitive data help keep your organization more secure. In addition, Exchange 2013 provides flexible options for moving to the cloud.

Migrating to Exchange 2013, however, presents changes to your infrastructure. This paper discusses how the migration affects your infrastructure and topics to consider, in particular:

- Securing remote, BYOD, and mobile device access.

- Readying your infrastructure for server role consolidation, IPv6, and virtualization, and configuring your network.

- Providing a safe and seamless user experience in a dynamic environment of migrations, updates, and heterogeneous mail systems.

- Supporting multiple data center deployments for disaster recovery.

Securing Remote, BYOD, and Mobile Device Access

The age of the corporate PC as the only device for accessing email is over. Migrating to this next version of Exchange provides an excellent opportunity to define your remote, BYOD, and mobile device access strategies.

Securing remote access

Legacy mail systems supported a single remote access solution, the dreaded VPN. Exchange 2013 supports perimeter authentication, which provides the same security as the VPN, but without the client and end-user software. By taking advantage of perimeter security, you can rest assured knowing that no unauthorized user will ever be able to connect to your Exchange server.

The need for security at the Exchange perimeter is still prevalent, however, and technology that replaces the discontinued Forefront Threat Management Gateway (TMG) needs to be used to provide firewalling, application security, and pre-authentication.

F5® BIG-IP® Access Policy Manager® (APM) provides an in-depth security model that goes well beyond the traditional username and password access method. By being able to interrogate Active Directory for security attributes (including a user's ActiveSync profile settings), inspect the client device, and build flexible access rules, BIG-IP APM protects Exchange from attacks that the typical VPN cannot.

Securing BYOD and mobile device access

People are increasingly using devices other than the corporate PC to check email. These devices vary in form factor and operating system, as well as ownership. No longer is simple username and password an acceptable authorization strategy when these devices are being used.

Access levels need to be granted based upon the client device as well as the client identity. For example, to determine the level of access to grant a specific user, it must first be determined if the mobile device connecting to the Exchange 2013 system is corporate owned and virus free.

F5 solutions can build a rich network security policy that grants different levels of access to the Exchange 2013 environment based upon a wide set of client-side and server-side criteria.

Readying Your Infrastructure and Configuring Your Network

Major architectural changes to the Exchange server roles will require a change in your network architecture that is different from Exchange 2010, 2007, and 2003 or IBM Lotus Notes. This is also an opportune time to prepare your network for the future, including IPv6, virtualized deployments, and optimization of your network configuration.

Properly architecting your network

In Exchange 2013, server roles have been consolidated from four to just two: Client Access server (CAS) role and Mailbox server role. This consolidation results in a clear distinction in network activity for each—the CAS servers act as proxies and the Mailbox servers act as endpoints. Therefore, it is necessary to plan and architect the network to fit Exchange 2013, not the other way around.

The flexibility F5 products offer in a network architecture (for example, VLAN, route domains, tagging, and an IPv4-to-IPv6 gateway) can enable a range of architectures that effectively and optimally deliver Exchange traffic without the need to purchase multiple devices.

When planning a move to Exchange 2013, it's wise to consider what other significant changes to network design may occur during the expected lifecycle of this version of Exchange. For example, if you plan on moving to IPv6 or to a network virtualized environment before upgrading Exchange again, can you implement those enhancements without having to rebuild the Exchange deployment from the ground up? F5 provides you with an IPv6 gateway or a network virtualization gateway that would allow you to migrate over to those new technologies without downtime or rebuilds.

Consolidating your infrastructure

Exchange 2013 has been designed to take advantage of consolidation in server roles and hardware. These benefits, in both cost and complexity, also extend to the network. Maintaining separate devices for each network responsibility is a cumbersome and time-consuming process that is prone to error.

The F5 solution combines local and wide area high availability, scalability, performance, and security all in the same device.

Configuring your network

Properly securing and optimizing the multiple network protocols within Exchange 2013 often means a large and complex configuration. Each protocol is different, and attempting to apply an umbrella network profile to cover all is going to result in an inefficient, and possibly insecure, network for Exchange 2013.

F5 iApps™ technology provides the management interface to handle a complex and optimal configuration while making configuration incredibly easy. F5 iApps are designed to take the minimal set of information regarding the Exchange deployment from the Exchange administrator and dynamically and quickly build the configuration. F5 has done the work to identify and build the best network configuration for all Exchange client types into the F5 Exchange iApp, thereby lessening the amount of work administrators need to do and drastically reducing the potential for misconfiguration errors.

Providing a Safe and Seamless User Experience in a Dynamic Environment

Heterogeneous and dynamic conditions, such as multiple mail systems, employees spread around the world, and mergers and acquisitions add to the challenges of managing mail systems, maintaining a seamless user experience, and protecting your organization's data during a migration.

Managing multiple mail systems during migrations

Unlike most application upgrades that use an abrupt, "no going back" cutover, a properly planned mail system upgrade can include old and new mail system coexistence. This results in a smooth migration in which users' mailboxes are moved over in phases. To accomplish this, your network needs to have the capacity and intelligence to manage multiple mail systems operating independently with distinctly different network footprints.

With true layer 2–7 networking engines, a single BIG-IP® device can manage the networks of long-living and multiple coexisting mail systems.

Building for change and flexibility

Enterprises rarely have the luxury of a single, homogenous, and static mail system. With a mix of local, remote, and increasingly international workforces, diversity in employment classifications (such as employee or contractor) and constant change with mergers and acquisitions, organizations need to allow for flexibility in the mail system. These realities require the use of a hybrid deployment model.

A hybrid deployment can be coexisting multiple versions of Exchange on-premises or it can be adopting a hosted version of Exchange, such as Office365, or both. Two examples of hybrid deployments are: 1) an organization running Exchange 2007 that decides to upgrade to Exchange 2010 or 2013, and 2) an organization running Exchange that decides to move to Office365. For many, the move is gradual, first moving to online message archival, SPAM filtering, or malware detection and eventually moving the actual user mailboxes.

A properly architected mail system should be able to provide the flexibility to support heterogeneous environments while maintaining a consistent end-user experience. This includes a single URL access, regardless of where the user's mail system resides.

The F5 solution provides single URL access—one path for organizations using both Exchange servers on-premises and Office365. Every user in the organization is identified and seamlessly connected to the Exchange environment where their mail is hosted.

For example, an organization with Exchange 2007 on-premises that federates its existing Active Directory with Office365 and upgrades to Exchange 2010 must install an Exchange 2010 server on-premises. As the organization migrates users to Office365, a given user's mailbox will move from on-premises to the cloud. Alternately, the organization may choose to designate some users' mailboxes to originate in Office365 and other users to maintain on-premises mailboxes and never move to the cloud. Regardless of the type of hybrid scenario, both the end-user experience and the complexity of administrating the process are affected by the need to reliably connect users to their mailboxes.

The properly architected network will seamlessly route users regardless of premises (on-premises or cloud) and regardless of the Exchange version.

Providing a seamless user experience

Upgrades and migrations mean that a specific user's mailbox will move from the old mail system to the new. This is compounded when the new system, such as Exchange 2013, supports multiple access methods and protocols. If not planned appropriately, this can create a nightmare for Exchange administrators who are forced to maintain a large set of namespaces for each specific user based upon the user's mailbox location and access and protocol and client device.

The F5 solution enables a true single namespace that not only spans Exchange 2013, but your organization's legacy and hybrid deployments as well. Imagine having a single URL to hand out to all end users, regardless of what device they are using, what access protocol they are using, or what system their e-mail resides on (whether it is legacy, Exchange 2013, or Microsoft Office365).

Supporting Multiple Data Center Deployments for Disaster Recovery

Traditional disaster recovery for e-mail systems required expensive, inefficient, and manual tape backup systems, which were prone to long delays and data corruption in times of restoration.

Exchange 2013 uses the concept of live, wide-area replicas as a means of having real-time backups ready at all times. Multi-site deployments make more sense than ever with Exchange 2013, as does the need for wide-area network intelligence and optimization. With the F5 solution, mailbox replication is optimized (including compression and acceleration), and support is provided to intelligently manage traffic to the multiple entry points in a multi–data center deployment.

More Information

To learn more about F5 solutions for Microsoft Exchange, visit the **Microsoft Exchange Server Solutions** page or search **f5.com** for the following resources.

Guide

F5 Deployment Guide for
Exchange 2010 and 2013

Datasheet

BIG-IP Access Policy Manager

Blogs

Comparing BIG-IP APM Deployment
and Microsoft TMG

Load Balancing the ADFS Farm:
Using BIG-IP LTM to Upgrade to
Exchange Online