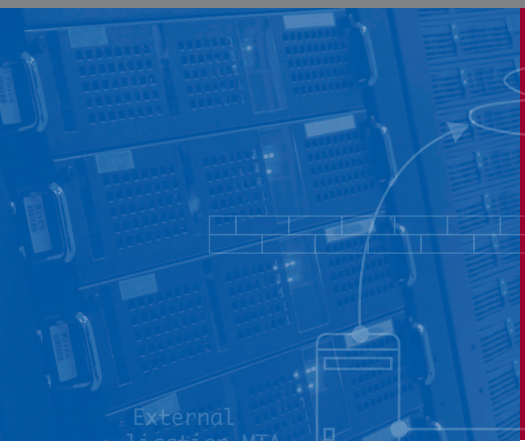
WHITE PAPER



The Importance of an Email Backbone for Microsoft Exchange and Office 365

Gregory Shapiro, VP and CTO

SENDMAIL®

Overview

Microsoft Exchange is the dominant enterprise email system across all organizations.[1] Most large organizations use Exchange on-premises due to the complexity of email network topology and the immaturity of cloud service offerings. The Gartner Position on Cloud Email, published June 1, 2012, found, "At the start of 2012, 6% of enterprise email users were using public cloud email. At least 75% of these organizations, however, have fewer than 500 users." From that, we can surmise that less than 2% of large enterprise organizations, those with 5000 or more users, have moved to a public cloud offering such as Office 365's Exchange Online.

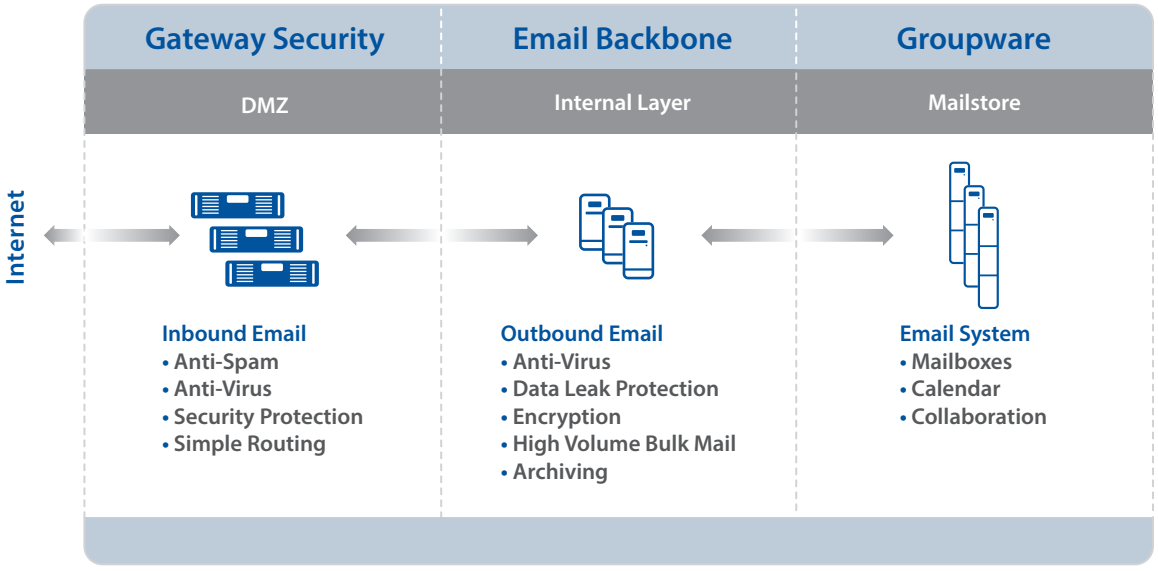
"This paper explores how an on-premises email backbone not only helps enable that migration to the cloud, but also explains why a backbone is required even after the migration is complete."

However, that reality is changing quickly as organizations start to look at migrating most, if not all, of their users into cloud-based offerings, particularly Office 365 from Microsoft. The aforementioned Gartner position predicted, "By the end of the decade we believe cloud email will account for about 65% of the enterprise email market."

This paper explores how an on-premises email backbone not only helps enable that migration to the cloud, but also explains why a backbone is required even after the migration is complete. It also offers guidance on best current practices for an on-premises email backbone for groupware services housed on-premises, in the cloud, or in a hybrid mixture of the two.

The Email Backbone

The first step in understanding the need for an email backbone in an Exchange environment is to understand what an email backbone provides and the best practices for deploying that backbone. That deployment would consist of three layers as shown in the figure below.



The first layer provides gateway security and hygiene services such as anti-spam, anti-virus, IP reputation, recipient validation, simple policy protection, and routing. It can exist in an on-premises DMZ or is one of the easiest layers to outsource to the cloud. Spam and virus filtering technologies have become commoditized and there is minimal security risk in having a third-party filter inbound email before delivering it to the end-user groupware mailbox. From an OPEX perspective, the hardware required to manage the gateway filtering function can be eliminated along with the costly maintenance, support, and management of those systems.

The second layer, also known as the internal layer as it is meant to live on the internal corporate network, provides the email backbone. As the backbone, it handles transit of all inbound and outbound mail. Inbound mail functions include complex policy-based routing, encryption, outbound anti-virus scanning, and additional inbound protection. As the outbound relay, it is responsible for enforcing outbound policy control with deep content inspection, whether for corporate governance, data leak protection, or compliance/regulatory control. This layer is also responsible for routing and queuing mail from both the groupware layer as well as machine-generated email.

The third layer is the groupware layer in which the end-user mail store, e.g., Microsoft Exchange, resides. The Groupware Layer (Microsoft Exchange, IBM Lotus Notes, etc.) has proven to be more technically challenging to migrate to the cloud, but it also provides the greatest ROI—some enterprises dedicate up to 95 percent of their IT messaging support team to manage this layer. The ROI that can be achieved by moving this layer to the cloud often outweighs some of the perceived security implications.

The gateway security and email backbone layers may be logically split to provide separate messaging channels for inbound, outbound, and machine-generated (e.g., application) mail.

The Need for an Email Backbone

As discussed, commoditization and reduced risk has made moving the gateway security layer to the cloud the easiest to achieve. Office365's Exchange Online offers a way to move Exchange groupware services into the cloud, as long as the limitations and security risks of doing so are acceptable (see appendix). However, the email backbone itself is not suited to move the cloud. Gartner points out, "Companies have found that cloud services lack the flexibility to support custom deployments and are unable to meet specific security, content control and application integration needs."[2] These concerns include the ability to meet compliance and regulatory needs, access forensics (logs, tracking, auditing), specify diverse policy-based routing, enforce change management/control, and ensure security requirements such as configuring mandatory TLS, and having local access to corporate data and systems of record (e.g., directory) for policy decisions and content modifications.

> "Companies have found that cloud services lack the flexibility to support custom deployments and are unable to meet specific security, content control and application integration needs."

Moving to the cloud further restricts usage and control, presenting the need for a hybrid infrastructure with an on-premises email backbone. With this in mind, this leaves three scenarios for architecting an on-premises backbone infrastructure with Exchange:

1. Keeping the Exchange groupware services on premises.
2. Moving a portion of your user population to Exchange Online.
3. Moving all users to Exchange Online.

With an on-premises Exchange environment, the first scenario, the backbone layer provides the needed policy and routing functionality described above. Note that although Exchange does provide basic policy control via Transport Hub rules, those policies are limited in both conditions & actions and Exchange does not support more than 100 transport rules, each limited to 4000 characters.[3] It can also be useful for preventing mail storming by enforcing rate limiting on both incoming and internal mail flows into the Exchange servers.

In the second scenario, the backbone has the additional challenge of performing policy based routing to support a segmented workforce under a single corporate identity. In other words, having a consistent email branding @company.com with delivery to multiple mailbox storage locations depending on the recipient's department, role, location, or other criteria. This ability is also useful in merger situations that require all employees to begin using one corporate identity before merging their separate mailbox environments.

The third scenario, in which all mailboxes are in the cloud, is interesting in that it may lead you to believe that no on-premises infrastructure is necessary. However, in most, if not all, organizations, human-generated email is less than 50% of the mail transiting the email backbone. Machine-generated email from hundreds, possibly thousands, of email-enabled applications and systems, many of which are hidden from IT visibility, generate more then half of the email backbone traffic. These machine-generating applications require on-premises infrastructure as the cloud may not be able to meet the integration requirements of a number of difficult to integrate applications. Consider, for example, applications that do not know about MX records; or hard code a hostname, or worse an IP address, to contact; or only contact the first IP address returned on a hostname lookup. These applications may also not deal well with latency and availability issues (i.e., may not have queuing abilities or robust timeout handling), necessitating the need for a local submission server. Finally, these applications may not have external network access to connect to a remote infrastructure or may be routing messages to other on-premises applications or systems, making a round trip through the cloud cumbersome and inefficient.

Although a topic for another paper, moving these applications to the cloud may not be feasible. "If the application has years of accumulated and poorly documented business rules embedded in code, and a proliferation of subtle or poorly understood interdependencies with other systems, the risks of "breakage" when the legacy application is migrated or retired make this a less attractive choice for early cloud adoption."[4] Additionally, applications in the cloud may require opening up external network access to expose internal databases and systems of record.

"If the application has years of accumulated and poorly documented business rules embedded in code, and a proliferation of subtle or poorly understood interdependencies with other systems, the risks of "breakage" when the legacy application is migrated or retired make this a less attractive choice for early cloud adoption."

For more information on the topic of machine-generated mail, see the Sendmail whitepaper, *"The Impact of Machine-Generated Messages on Enterprise Email Infrastructure."*

Luckily, Microsoft recognizes the need for on-premises email backbone infrastructure, even if just for address rewriting, and has provided features for organizations in the last two scenarios in which some or all user mailboxes are in the cloud-based Exchange Online. Microsoft Exchange Online for Enterprises Service Description[5] discusses configuration for both inbound email via proper MX record configuration and outbound email using the Exchange Online Outbound Smart Host feature.

Choosing the Right Backbone

With the requirement for an email backbone established, the final step is determining the best backbone infrastructure to fulfill that need. This can be accomplished in one of three ways:

1	**Internal development via open source or internally developed MTAs, filters, and add-ons**	**2**	**Employing email security appliances, i.e., transforming point products to act as gateways**	**3**	**Using the Sentrion message processing platform**

Employing the internal development route will provide the lowest up front costs but the highest ongoing development and support costs. For the most simplistic case of creating a choke point between groupware, machine-generated email application servers, and inbound/outbound message flows, an open source MTA can be compiled and configured. However, once additional functionality is needed (e.g., rate limiting, policy, DLP, message tracking, reporting, DKIM, etc.), the complexity of finding other open source or point products or writing your own code to fit those needs, integrating them together to function as a unit, and then managing them across multiple servers with configuration control is a daunting task to undertake and will require email gurus, coders, and a large system administration staff to maintain. A large investment in time and resources will be spent to build, maintain, troubleshoot, and support the functionality found in a modern messaging platform.

Using an email security appliance as the onsite gateway provides more of the tools necessary to implement policy and control over the mail flow but comes at the cost of locking your abilities down to only what is provided by that security appliance. Email security appliance point products provide the basic functionality necessary in a closed solution meant to solve specific problems and limiting the configurability to satisfy those problems. Branching out from these limitations is impossible or unsupported in most, if not all, cases. Adding that additional functionality via additional products will still require an in-house integration, resulting in a complex interconnection of appliances and software from multiple vendors to manage. It will not provide a simple backbone with a single management interface for unified configuration and policy control. Challenges will arise such as alternative routing of different classes of mail that require different hygiene and policy handling. End-to-end message tracking and reporting will be difficult to achieve. Finally, a multi-vendor troubleshooting session when something does go wrong can be frustrating.

The Sentrion Appliance is an open platform for solving the complex problems found in modern email infrastructures. Because the Sentrion is meant to cover all of the complex issues, it is perfectly suited to handle the needs of providing onsite full-content message inspection to enable policy-based control and delivery with unlimited actions on message body, header, and all attachments, as well as complete monitoring and reporting, etc. If functionality isn't included with the base system, the platform allows for extensibility through custom policy extensions, integrated third party applications via the Applications SDK, custom reporting via Premium Reporting, powered by Splunk, etc. Visit the ***Sendmail Sentrion Application*** store for further details.

Conclusion

Regardless of whether Exchange is deployed on-premises, in the cloud using Office 365's Exchange Online, or a hybrid of the two, an on-premises email backbone is a fundamental requirement for a modern messaging infrastructure. That backbone can handle an organization's compliance and regulatory needs, provide access to forensics (logs, tracking, auditing), implement diverse policy-based routing, enforce change management/control, and ensure security requirements, as well as provide transit services to on-premises machine-generated mail. The Sentrion message processing platform is the best-suited choice for providing that modern email backbone.

Appendix: Office 365 Exchange Online Limitations

Migrating portions of your mail infrastructure to the cloud requires compromises based on the cloud provider's limitations. Those limitations can come in the form of usage constraints and your ability to configure and control your environment as needed. It is important to factor these considerations in when deciding which portions of the mail infrastructure make sense to move to the cloud.

The Sendmail whitepapers, *"Moving to the Cloud: Important Things to Consider Before Migrating Your Messaging Infrastructure to the Cloud"* and *"Important Information for Enterprises Moving Email to the Cloud"* go into detail about the risks, limitations and compromises necessary. However, as it relates to the email backbone, lets take a look at some of the limitations of Microsoft's Office 365 offering described in Office 365's Message and Recipient Limits. [6]

These outline a number of limits you must impose to make use of their solution. Many are likely easy to cope with, e.g., no more than 125 attachments per message or 255 characters in a Subject header. However, some will impose severe limits on both users communicating collaboratively as well as mail generating applications:

- Office 365 does not allow a message, including headers, body, and all attachments, over 25 megabytes. This will require users to find other means of sharing files, possibly outside of policy control of the organization (e.g., external file sharing sites such as DropBox).
- Mailings can have at most 500 recipients and a sender can send mail to at most 1500 recipients per 24-hour period and only 30 messages per minute. While this may seem reasonable for a human sending mail, it is an unreasonable limitation to place on mail generating applications. Other circumstances can

also make this risker. For example: "Buggy calendar code creating cancellation request storms, leading to inoperable mailboxes due to users going over the 500 messages per day sending limit." [7]

- If an attempt is made to overcome those recipient limits via a static distribution group, new restrictions introduce speed bumps in mail delivery once the distribution list reach 5000 members. It also introduces a new maximum message size of only 2 megabytes.
- An organization can only have up to 100 transport rules. Transport rules are Office 365's form of policy control and routing. This should be compared to the number of mail routing (e.g., MTA mailertable) entries, mail access table entries (e.g., MTA access database), and distinct policy engine policies in use in your infrastructure. The limit of 100 rules will likely be insufficient to suit an organization's needs.

Taken all together, these limitations encourage the use of a hybrid solution in which the person-to-person groupware layer may be appropriate to place in the cloud but the email backbone, with its ability to handle flexible policy and routing control, configurable limits, and ability to handle application generated email, should remain on-premises or in a tightly coupled private cloud under the organization's control. In fact, you'll find exactly that advice in the Office 365 documentation[8] in which they recognize the need for machine-generated email to use an on-premises mail server.

Footnotes

1. The Museum of Email and Digital Communication
   http://email-museum.com/reports/ferris-research-completes-most-comprehensive-survey-of-business-email-systems-to-date/
2. Matthew W. Cain, "Combining On-Premises and Cloud E-Mail: Perfect Together?",
   Published: 5 April 2011, Gartner ID: G00212093
3. Transport Rule Limits, Message and Recipient Limits, http://help.outlook.com/140/dd630704.aspx
4. Vivek Kundra, U.S. Chief Information Officer, "Federal Cloud Computing Strategy," February 8, 2011
   http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf
5. http://www.microsoft.com/en-us/download/details.aspx?id=13602
6. http://help.outlook.com/en-us/140/dd630704.aspx
7. Matthew W. Cain, "Users Share Problems With Office 365 Email Migration",
   Published: 26 April 2012, Gartner ID: G00231772
8. http://help.outlook.com/en-us/140/Ff381292.aspx

About Sendmail, Inc

Sendmail provides enterprises with global email connectivity, routing, and message delivery between people, systems, and applications. The Sentrion Email Infrastructure Platform reduces enterprise IT complexity and lowers the cost of integrating critical message content with business processes. Since 1982, thousands of enterprises around the world have relied on Sendmail open source and the award winning Sentrion hard and virtual appliances, and its suite of applications, for intelligent email backbone and secure message gateway infrastructure. Unlike proprietary email-security appliances, Sentrion provides full-content inspection and policy-based delivery for all collaborative groupware and machine-generated email, whether deployed on-premises, in-cloud, or via mobile devices. Sendmail is headquartered in Emeryville, CA with sales and support offices throughout the Americas, Europe, and Asia.

Sendmail, Inc.
6475 Christie Avenue, Suite 350, Emeryville, CA 94608 USA

Tel: +1-888-594-3150 | Fax: +1-510-594-5429
Email: info@sendmail.com
www.sendmail.com

Copyright © 1998-2012 Sendmail, Inc. All Rights Reserved. All other company and product names may be trademarks or registered trademarks of their respective organizations. WP-01-0812