ActiveAnswers

iss solutions

april 2003

solution overview

Sendmail Mail Transfer Agent for Linux on hp ProLiant servers

abstract: This solution guide describes how Sendmail Mailstream Manager, which includes the Sendmail Mail Transfer Agent (MTA), can be used with Linux on HP ProLiant servers to offload and protect corporate groupware servers. It also provides a brief overview of the functions of groupware servers – such as Microsoft Exchange Server, IBM/Lotus Domino and Novell GroupWise – then presents the Sendmail MTA solution.

contents

notice

The information in this document is subject to change without notice.

april 2003
P/N 04/2003 - 1

introduction

Businesses today rely more on e-mail communications than ever before. Internally, e-mail and other collaborative electronic tools are used by employees to share information. E-mail is also used to communicate externally to customers and suppliers. This external transfer of e-mail is typically accomplished through the use of a connection to the Internet, which allows two-way communication with anyone else who also has access to the Internet. However, as much as using e-mail to communicate over the Internet facilitates communication with customers, partners, and suppliers outside of the corporate network, there are risks associated with exposing e-mail servers directly to the Internet. If companies are not careful, they could open their corporate e-mail infrastructure to the threat of external attacks, which many e-mail systems are unprepared for. Sendmail, Inc. and HP have a solution that not only improves the performance of corporate e-mail systems, but also provides protection for internal e-mail systems from external security threats.

groupware solutions

Groupware is a term coined to describe systems that enable groups of individuals (e.g. employees of a company, a specific department, members of an organization) to work together over a computer network. Groupware solutions include products such as Microsoft Exchange Server, IBM/Lotus Domino, and Novell GroupWise. These systems typically include e-mail and PIM (Personal Information Manager) functions, such as contacts and calendar. In general, groupware solutions provide the tools to enable users to work together by sharing information: project data, meeting schedules, contact names, e-mail, etc. Many companies rely on groupware solutions for their e-mail and other internal and external electronic communication needs. However, functionality, not performance or security, is the goal of groupware. Depending on groupware to protect the integrity of the enterprise mail system from Internet threats and to maintain the confidentiality of proprietary content may seriously compromise network security.

For more information on the three groupware solutions mentioned, visit their websites:

Microsoft Exchange: http://www.microsoft.com/exchange

IBM/Lotus[1] Domino: http://www.ibm.com/domino

Novell GroupWise: http://www.novell.com/groupwise

[1] Domino was originally a product of Lotus, which was acquired by IBM.

Groupware servers often contain confidential information: user IDs, passwords, project data, confidential employee information, etc. This type of information warrants a high level of security. If a groupware server is exposed outside the firewall - to allow easier e-mail connectivity, serve as an offsite backup, etc - sensitive data may be compromised. It is strongly recommended that any server containing confidential information be separated from the Internet by not only the corporate firewall, but also by a gateway server. In the case of a groupware server that requires e-mail access to the Internet, that gateway server could run Sendmail, which was built to handle these security and performance requirements. This enables the groupware server to still have e-mail access to the Internet, but protects the data it contains by keeping it behind the firewall or gateway server, and allowing no direct connection from the Internet.

In other cases, the intent of an attack is not to steal information, but simply to disrupt a server or network. A Denial of Service (DoS) attack is an attempt to overload a server or network by flooding it with continuous useless traffic. Groupware servers are not designed to recognize or prevent this type of attack. As previously stated, it is recommended that groupware servers be behind the corporate firewall and if possible, separated from the Internet by a gateway server that can identify and thwart DoS attacks.

High utilization is another issue that groupware servers may pose to administrators. With ever-increasing e-mail volumes, additional groupware servers may be required to handle the load. Add to that the possibility of unauthorized use of server resources by someone outside the company. Unsolicited bulk e-mail, or "spam," is a growing problem for all Internet-attached e-mail systems. Spam directed at a groupware server's users is only part of the problem. Spammers may also exploit security vulnerabilities in groupware servers to relay large amounts of e-mail. Unauthorized use of these "open relays" can result in higher than normal processor and disk space resource utilization, causing delayed or bounced legitimate e-mail. In addition, victims of open relays often find themselves mistakenly identified as the spammers, resulting in blacklisting that can prevent users from sending legitimate e-mail.

Sendmail background[2]

Sendmail is a leading provider of powerful e-mail systems for enterprise and service providers. With proven technology and unmatched expertise, Sendmail works with customers to address their most complex messaging challenges. The result is dependable e-mail infrastructure that is easy to manage and built to grow.

Sendmail is an e-mail pioneer, having played a key role in the evolution of e-mail and the Internet from the very beginning. The *sendmail* Mail Transfer Agent (MTA), the de facto standard implementation of the Simple Mail Transfer Protocol (SMTP), has been the foundation of Internet messaging for more than 20 years – and it still powers more than 60 percent of the Internet's mail domains. Recently honored by the Smithsonian Institution for its contributions to the advancement of information technology, Sendmail remains a leading contributor to the ongoing evolution of e-mail and the Internet.

[2] The Sendmail background information used in this guide was obtained from text and documents available on the Sendmail website, http://www.sendmail.com.

Today, Sendmail powers four times more Internet mail domains worldwide than its largest competitor. In addition, 9 of the Fortune 10 and 84 of the Fortune 100, as well as 29 of the world's 36 largest Internet Service Providers rely on Sendmail technology.

Sendmail offers the Internet's only set of solutions whose core technology, *sendmail*, helped define how Internet mail operates. It is considered the benchmark for open standards e-mail and Internet mail innovation. In addition to robust and secure e-mail routing, Sendmail, Inc. delivers simplified administration and management tools, encryption and authentication, scalable POP/IMAP message stores, LDAP services, mail network unification and spam and virus filtering support.

Sendmail's e-mail routing, storage and access solutions can be combined in a number of ways to address the communications needs of enterprises and service providers worldwide. The Sendmail Mailstream Manager solution offers essential e-mail applications and services that ensure reliable and secure flow of e-mail. The Sendmail Mailcenter solution provides the only complete suite of bundled, fully integrated, rapidly implemented and affordable e-mail applications for e-mail routing, storage, and access from a variety of devices, including webmail and wireless. Sendmail High Volume Mail Solution offers an e-mail system designed to deliver subscriber-based mass e-mailing of time-sensitive, opt-in personalized information.

This guide focuses on the use of the Sendmail Mailstream Manager in conjunction with an existing groupware server implementation. In this scenario, Mailstream Manager is used to address two issues concerning groupware servers: security and performance.

Sendmail's Mailstream Manager consists of several components that work together to create a complete solution for managing and securing the content and flow of e-mail into and within an enterprise. In the groupware + Sendmail scenario, the following components can be used:

- **Managed Switch** – the heart of the system, the Mail Transfer Agent (MTA). Managed Switches route messages through the network toward their final destination. In addition to performing e-mail routing, queuing, and anti-relaying, they handle encryption and filtering of incoming and outgoing messages, based on the configuration options chosen.
- **Administration Console** – web-browser-based management tool that controls the Managed Switches in the network from a single, secure remote console. The Administration console gives administrators the ability to view or change the configuration of any Managed Switch in the network. The console also provides activity logs, automated alerts and notifications, and management reports. It also simplifies scaling the e-mail network by allowing IT staff to add, configure, deploy and manage additional mail routing servers from a centralized console.
- **Anti-Virus Filter** – scans messages at the server level, incoming and/or outgoing, eliminating viruses before they reach the client systems or are able to spread throughout the enterprise network. Virus updates can be manual or automatic.

- **Anti-Spam Filter** – intelligent spam filtering solution. Allows an organization to monitor, manage and filter unauthorized inbound, outbound and intra-company e-mail. The anti-spam engine is trained with tens of thousands of messages – spam and legitimate e-mail – to identify and inventory what is spam and what isn't, increasing accuracy and reducing false positives. Once a message passes though the gateway server, the Anti-Spam Filter scans the header, message body and attachments to eliminate unsolicited e-mail. Messages that meet the threshold spam criteria can then be destroyed, redirected, quarantined, blocked or tagged, depending on customer preference.
- **Policy Enforcement Filters** – allow companies to enforce policies regarding the messages that flow through their e-mail systems. The Attachment Filter, Message Copier, Message Appender and Flow Control Filter provide administrators precise control of incoming and outgoing content and the ability to limit message size, limit server connections, copy and archive messages, add legal disclaimers, strip attachments and perform a variety of actions on messages based on corporate policy.

Sendmail Mailstream Manager instantly adds security, reliability and performance to groupware e-mail systems. It enables IT managers to easily monitor the entire e-mail network through a secure, remote console, gaining visibility on its operation. System administrators can change the settings on any Managed Switch and immediately view the results, adding real-time control capabilities to better run their networks.

For more information on Sendmail, the company, and its products, please visit http://www.sendmail.com.

Sendmail as MTA for groupware servers

As mentioned previously, groupware servers are not typically designed with security or performance as main concerns. Adding the Sendmail Mailstream Manager solution to an existing Internet-attached groupware e-mail system adds the security and performance that groupware servers, standing alone, are lacking, and that companies require to optimize their use of e-mail as a business-critical communications tool.

security

Using Sendmail's Mailstream Manager solution, e-mail system administrators can increase the security of an existing groupware e-mail system. Using Sendmail as a gateway between a groupware server and the Internet greatly improves the safety of the data contained on the groupware server. This keeps the groupware server safe inside the firewall, while the only communication allowed to reach the server through the firewall is from the Sendmail gateway. Combined with the Flow Control Filter, Sendmail MTAs can also manage the flow of e-mail into and out of an enterprise network, thwarting DoS attacks or e-mail harvesting attacks launched by spammers. Additionally, using the Anti-Virus filter on the Sendmail gateway stops viruses before they enter the network. Containing viruses before they reach the clients or their groupware server drastically reduces the incidence of desktop infection and further virus propagation.

performance

Using Sendmail's Mailstream Manager solution, e-mail administrators can increase the performance of existing groupware systems. When e-mail volumes are heavy, groupware servers may be strained under the load. This may lead system administrators to believe that additional groupware servers are needed to handle the increased load. A more cost-effective method is to offload the mail transport function from the groupware server to the Sendmail gateway.

Mailstream Manager's multi-layer and modular architecture allows user organizations to run redundant hardware to prevent a single component failure from immobilizing the entire network. The Mailstream Manager architecture includes optional onsite and offsite failover servers. This assures that in case of an internal or external failure, an alternate e-mail server can accept and queue e-mail for delivery, so the system does not lose any messages. When the regular e-mail system resumes operation, recipients will receive mail from the queue. During an outage, customers, business partners and even internal users will never see a message bounce. Many groupware systems such as Microsoft Exchange and Lotus Notes are preconfigured to bounce mail if they do not receive an immediate confirmation.

using Sendmail as MTA for IBM/Lotus Domino

According to an IDC report, IBM/Lotus Domino is the leader in the groupware marketplace, with a 49% share of the market. The closest competitor is Microsoft Exchange, at 39%.[3] However, the Domino server name is not as recognized as the name of the client application, Notes.

Of the three groupware servers discussed in this paper, Domino is by far the most flexible in terms of operating systems supported. There are versions of the Domino server for:[4]

- Microsoft Windows NT 4.0 operating system (using an Intel® processor)
- Microsoft Windows 2000 operating system (Server and Advanced Server editions)
- Sun Solaris Operating Environment 2.8/SPARC
- IBM AIX® operating system, Version 4.3.3x and 5.1
- IBM OS/400® V5R1 or later, using the IBM iSeries™ (formerly IBM AS/400®)
- IBM z/OS™ V2R6 or later, using the IBM zSeries™ (formerly IBM S/390®)
- Red Hat Linux®, Version 7.2 or SuSE Linux, Version 8.0 (using an Intel processor)

Unlike the graphical installers of the Windows/Mac versions of Domino, the Linux version of Domino is installed by means of a text-based install script. The server can be administered from Linux (web-based interface) or Windows/Macintosh (Domino Administrator application) clients; however the Notes client is only available for Windows and Macintosh, not for Linux.

[3] IDC market share numbers obtained from report at Worldwide Integrated Collaborative Environments Forecast and Analysis, 2002-2006: How Vendors Can Keep the ICE Flowing, http://www.microsoft.com/exchange/evaluation/compare/IDCICEReport/27600.htm

[4] Domino system requirements obtained from the IBM/Lotus Domino website at IBM Lotus Software - Notes and Domino 6, http://www.lotus.com/products/rnext.nsf/wdocs/30D0A92996C2955385256C4100650134

Domino uses two types of mail routing. For e-mail within the Domino domain (among multiple Domino servers), the server may use Notes routing (default) or SMTP. For e-mail destined for outside the Domino domain, the server will use SMTP. To accomplish SMTP routing to the Internet, e.g. using a Sendmail MTA, the Configuration Settings document on the server(s) must contain the name of the Sendmail server in the "Relay host for messages leaving the local Internet domain" field. Each Domino server must also have the setting "SMTP used when sending messages outside of the local Internet domain" enabled. These two settings will force the Domino server to send all Internet e-mail through the Sendmail server.

For more information about IBM/Lotus Domino server, including links to downloadable trial versions of Domino and Notes, visit http://www.ibm.com/domino. For links to downloadable documentation specifically for Domino v6, visit IBM's Domino 6 Documentation Library. For HP ActiveAnswers information on IBM/Lotus Domino, see Lotus Domino on the HP website.

using Sendmail as MTA for Microsoft Exchange Server

Microsoft Exchange, according to the IDC report previously referenced, is the second most popular groupware solution. Exchange servers come in three distinct versions:

- **Exchange 2000 Server** – targeted at the messaging and collaboration needs of small- to medium-sized businesses.
- **Exchange Server Enterprise** – for larger, enterprise corporations that require the use of multiple storage groups and multiple databases.
- **Exchange 2000 Conferencing Server** - provides data conferencing with application sharing and multicast video conferencing for organizations of all sizes. Must be deployed with Exchange 2000 Server or Exchange 2000 Server Enterprise (essentially a conferencing add-on).

Exchange 2000, which runs only on Windows 2000 Server or Advanced Server, integrates with Windows 2000 Active Directory, provides scalable/multiple databases, and two-way and four-way clustering for high availability. However, Exchange does not include its own SMTP server, and instead relies on the SMTP service which installs by default with Windows 2000 Server and Advanced Server.

When configuring Exchange to work with Sendmail, you must create an "SMTP connector" on the Exchange server. This virtual device (or devices) can then be pointed at an external server, such as a Sendmail mail-hub or gateway server, which is designated as a "smart host." Using the smart host approach, the Exchange server passes all e-mail to the smart host without verifying the destination domains, leaving that task for the smart host. This boosts performance by allowing the Exchange server to concentrate on internal e-mail traffic.

For more background information on Microsoft Exchange, visit their website at http://www.microsoft.com/exchange. To obtain a trial version of Exchange, visit http://www.microsoft.com/exchange/evaluation/trial/default.asp. For more information on deployment and configuration, go to the Microsoft TechNet Exchange guide at: www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/default.asp and also refer to ActiveAnswers documentation at Microsoft Exchange Server on the HP website.

using Sendmail as MTA for Novell GroupWise

Novell's GroupWise is typically considered a NetWare-based groupware solution. However, GroupWise 6 will run on Windows 2000/NT as well as NetWare 5/6. The following GroupWise 6 system requirements are taken from the Novell GroupWise website:

> System Requirements: Novell NetWare 5 or 6 (with Novell eDirectory) or Microsoft Windows 2000/NT. To implement GroupWise 6, you do not have to upgrade eDirectory, but some features (LDAP authentication and LDAP retrieval of S/MIME public keys) will require eDirectory 8.5.[5]

According to Novell's documentation, GroupWise is dependent on Novell's eDirectory (formerly NDS or NetWare Directory Services). All GroupWise components, such as domains, post offices and user accounts are all configured through eDirectory. The features of GroupWise include things such as e-mail (POP, IMAP and web mail support), calendar and scheduling, task management, and support for server side or client-side LDAP (Lightweight Directory Access Protocol).

Unlike the Exchange and Domino solutions, GroupWise, by default, does not support Internet e-mail connections. To add this functionality, an extra module must be installed – the GroupWise Internet Agent – which is included on the GroupWise CD. To enable the Sendmail server to handle all external mail delivery, during installation or configuration of the Internet Agent, you must select the option "Send Outbound Mail through a Relay Host" and enter the IP address of the Sendmail server.

For more information about Novell GroupWise, including an available demo, see their website, http://www.novell.com/groupwise or ActiveAnswers documentation at Novell GroupWise on the HP website. Full GroupWise 6 documentation, including configuration information for the Internet Agent, is available at http://www.novell.com/documentation/lg/gw6/index.html

[5] Novell GroupWise system requirements obtained from the GroupWise website at http://www.novell.com/products/groupwise/sysreqs.html

selecting hardware for a Sendmail solution

With the understanding that every computing environment is different, some suggestions and examples of Sendmail solution configurations will be given. It is up to the administrator to review the recommendations and collect the data needed to properly "size" the hardware for the specific implementation. Two different environment types are discussed, the Small Business network and the Enterprise network, with high and low volume system examples for each.

sizing considerations

When planning a Sendmail installation, there are several important points to consider in order to properly size the hardware configuration.

- Expected mail volume – If the Sendmail system replaces an existing system, data should be available that provides a good estimate of the load the Sendmail system will be required to handle. If the installation is a new system, the system administrator(s) involved must create an estimate based on other data: who will be using the system, comparisons with other similar sites, etc.
- Need for fault tolerance – Is this system business critical, or could some downtime be tolerated? For the majority of corporations, e-mail has become an indispensable tool, making any unplanned downtime unacceptable.
- Throughput vs. processing power – For high message throughput, input/output (I/O) performance is critical. Using multiple hard drives, such as RAID arrays, or storage area network (SAN) storage, increases the I/O throughput, allowing a higher message volume. For running the Sendmail filters, such as Anti-Virus and Anti-Spam filters, memory and processing power are most important. Each server needs to be optimally configured for the intended task.
- Budget – Higher performance and higher fault tolerance come at a price. The need for performance and fault tolerance has to be weighed against the dollars available to spend. The spectrum ranges from one server handling all services (lowest performance, lowest fault tolerance, lowest expense) to multiple servers assigned to each service (highest performance, highest fault tolerance, highest expense).

small business network configuration

A small business network is assumed to be an organization or site that only requires one groupware server to handle all e-mail traffic, typically up to 500 clients. In this scenario, a single groupware server services clients from inside the firewall. The Sendmail gateway resides outside the firewall, and handles the delivery of all external e-mail. All incoming mail must pass through the gateway server, where it is scanned for viruses by the Anti-Virus filter and checked against the rule set of the Anti-Spam filter. All outgoing mail is checked against the rule set of the Policy Enforcement filters for things such as message size and content.

Figure 1 shows an example of a small business network configuration. In this example, the single groupware server uses the single Sendmail server as a gateway for all Internet e-mail. Two recommended configuration options are given below. The decision between these two options is to be based on customer e-mail usage patterns and high availability requirements:

- Low volume – one HP ProLiant DL380 G3 server to server as the mail gateway, with:
  - optional redundant power supply
  - one 2.8 GHz processor
  - two 36GB hard drives
  - 1GB RAM
- High volume – one ProLiant DL380 G3 server to server as the mail gateway, with:
  - optional redundant power supply
  - two 2.8 GHz processors
  - two 36GB hard drives
  - 2GB RAM
- Added redundancy – for each case, add one extra identically configured server for added redundancy. This configuration provides failover capability in case of server failure.

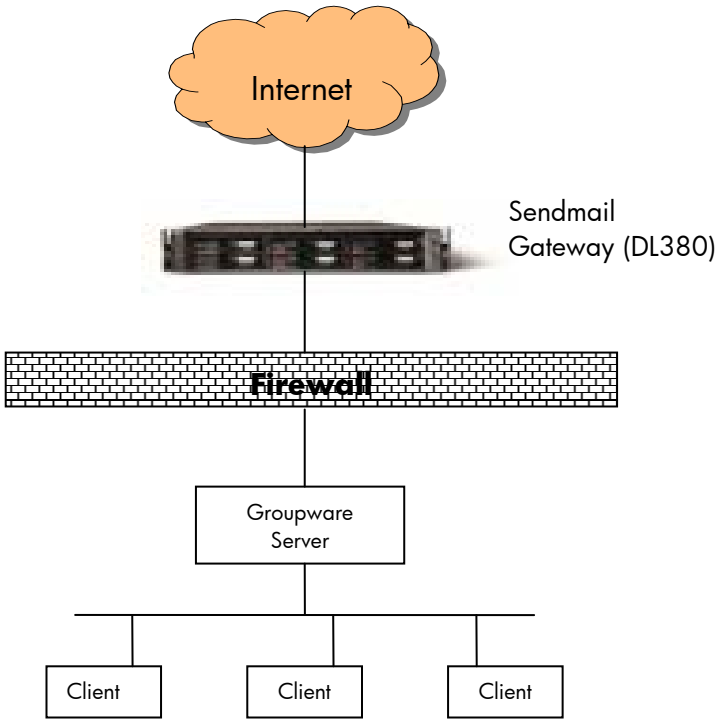

Figure 1. Small Business Network with Sendmail

enterprise network configuration

An enterprise network is assumed to be an organization or site that requires multiple groupware servers to handle all e-mail traffic, with typically more than 500 clients. In this scenario, multiple groupware servers service clients from inside the firewall. The Sendmail mail hub(s) reside(s) inside the firewall, and can be used for all internal e-mail delivery between groupware servers if desired. The Sendmail gateway server(s) reside(s) outside the firewall, and handle(s) the delivery of all external e-mail. All incoming mail must pass through the gateway server, where it is scanned for viruses by the Anti-Virus filter and checked against the rule set of the Anti-Spam filter. All outgoing mail is checked against the rule set of the Policy Enforcement filters for things such as message size.

Figure 2 shows an example of an enterprise network configuration. In this example, multiple groupware servers use one or more Sendmail servers as mail hubs inside the firewall, and one or more Sendmail servers as gateways for Internet e-mail. All Internet e-mail is sent by the internal mail hubs through one of more Sendmail gateway mail servers. Two recommended configuration options are given, each with complete redundancy.

- Low volume – two identically configured ProLiant DL380 G3 servers, one as the mail hub for outgoing mail, one as the mail gateway for incoming mail, each with:
  - optional redundant power supply
  - two 2.8 GHz processors
  - two 36GB hard drives
  - 2GB of RAM
- High volume – two identically configured ProLiant DL580 G2 servers, one as the mail hub for outgoing mail, one as the mail gateway for incoming mail, each with:
  - optional redundant power supply
  - four 2.8 GHz processors
  - two 36GB hard drives
  - 4GB of RAM
- Added redundancy – for each case, add two extra identically configured servers for added redundancy. This configuration provides failover capability in case of server failure.

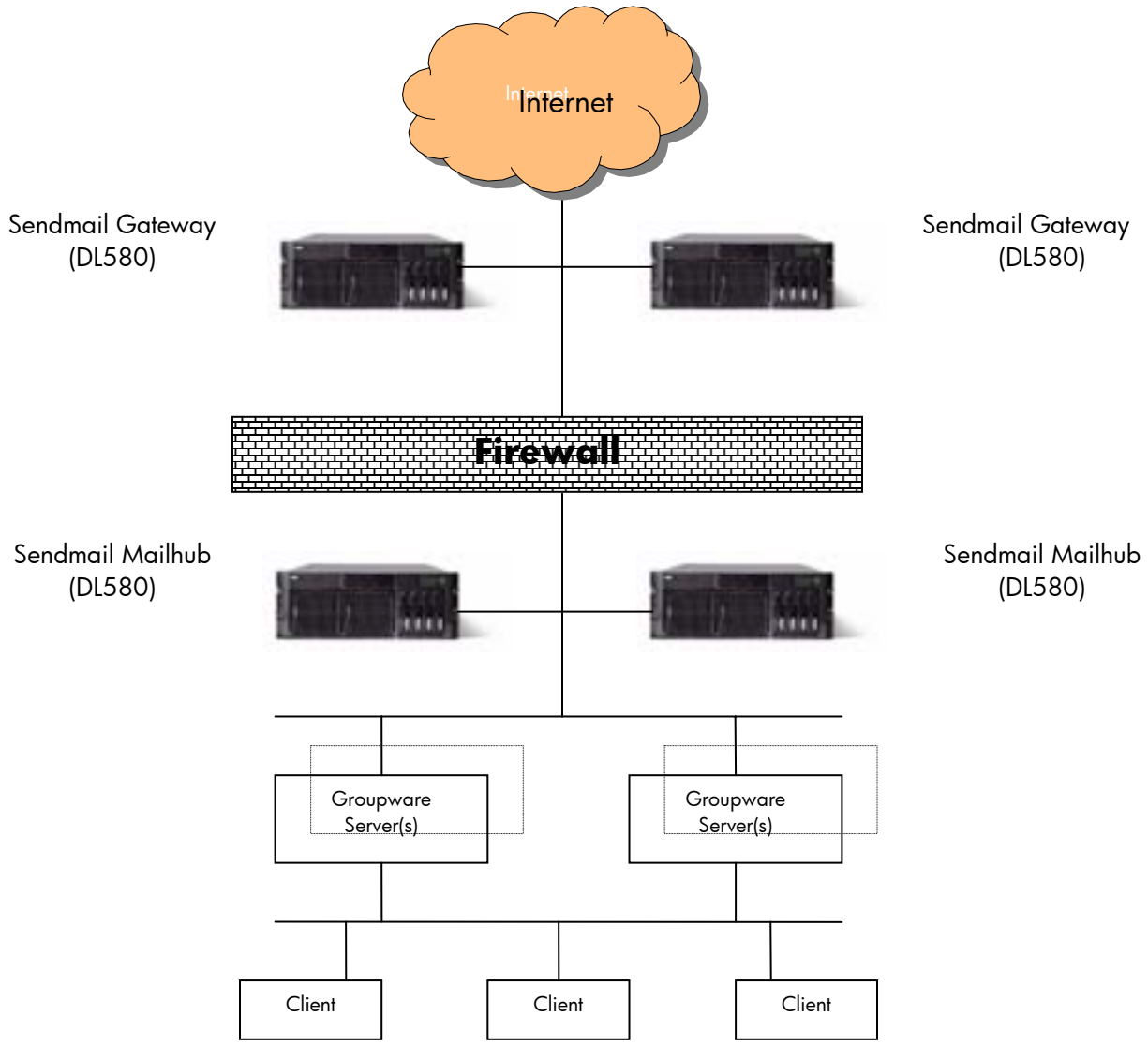

Figure 2. Enterprise Network with Sendmail

Another configuration example, using Sendmail's Mailstream Manager and ProLiant hardware can be accessed from the HP website, using the link - http://h18022.www1.hp.com/products/software/linux/mailmsg/mailstream.html . This downloadable document outlines a Sendmail Mailstream Manager configuration using multiple ProLiant DL360 G3 servers for redundancy and to spread the workload among multiple servers. For example, the virus scanning function has been separated out onto its own server, rather than residing on either the mail hub or gateway servers.

considerations for hardware configuration

Using these example configurations as a starting point, administrators can analyze the specific network needs and create the optimum configuration for their environment. Also, the modular nature of the Sendmail solution makes it simple to upgrade/extend the architecture. As any particular system's utilization grows, more servers can be added to distribute the workload. For example, a company may initially deploy a single server configuration. As e-mail volume increases, a second server can be added. If e-mail volume continues to increase, more servers can be added, simultaneously increasing the performance and fault tolerance of the system.

To reiterate, when designing a Sendmail solution and selecting hardware, keep these items in mind:

- Input/Output speed: As e-mail volume increases, the input/output (I/O) speed of the system becomes crucial. In particular, disk I/O can be a limiting factor in writing and reading data to and from mail queues. When selecting drives, be aware of the speed of the drives. For example, ProLiant servers now have 10K and 15K RPM disk drive options. The 15K RPM drives provide 26% faster data access, increasing the overall throughput capability.[6]
- Processor speed and single/multiple processors: Processor performance is most important for the server(s) that will be running Sendmail Filters, such as the Anti-Virus and Anti-Spam filters.
- Memory: Just as for processor performance, the RAM requirements are greater for the server(s) running Sendmail Filters.
- Fault tolerance: Consider the fault tolerance required for a given solutions against the available budget. On a single server, error correcting code (ECC) memory, a redundant power supply, multiple network connections, and mirrored or RAID drives can provide some measure of fault tolerance. Even when an entire Sendmail solution can exist on a single server, a second, redundant server greatly increases the system's fault tolerance. Beyond this, deploying multiple servers for each part of the solution (Mail Hub, Mail Gateway, Filters, etc.) increases performance and prevents the localized failure of any single server from causing the failure of an entire system.

[6] Both the 10K and 15K RPM Ultra320 SCSI drives provide a max transfer rate of 320MB/s. System throughput is a function of the transfer rate and the data access speed, especially when dealing with large numbers of small files. A link for more information is provided at the end of this document.

summary

As corporate e-mail volumes increase, administrators are challenged to find the most cost-effective way of increasing system performance to handle the load. At the same time, administrators are presented with increasing volumes of spam, viruses, and other security attacks. For networks relying on groupware servers for their e-mail communication, the most obvious solution, adding more groupware servers, may be the most expensive. Another more efficient solution can solve both issues with one product: Sendmail. Using Sendmail as the MTA for overloaded groupware servers reduces their workload while also keeping the groupware servers isolated from the Internet. The addition of Sendmail's virus and spam filters protects the internal e-mail servers and clients from e-mail messages that at best are useless, and at worst are potentially damaging. In addition, the policy enforcement filter makes it possible for companies to verify the contents of outgoing e-mail, including attachments, to ensure compliance with corporate e-mail policies. With the easy scalability of the Sendmail solution, these benefits are available for any size enterprise.

references

HP:

ProLiant DL360 G3: h18004.www1.hp.com/products/servers/proliantdl360/index.html

ProLiant DL380 G3: h18004.www1.hp.com/products/servers/proliantdl380/index.html

ProLiant DL580 G2: h18004.www1.hp.com/products/servers/proliantdl580/index.html

HP Ultra320 SCSI drive information:

h18004.www1.hp.com/products/servers/proliantstorage/drives-enclosures/hotplug-ultra3/description.html

Sendmail:

Sendmail info: www.sendmail.com

Sendmail/HP/Intel Solutions: www.sendmail.com/hpintel

Sendmail Mailstream Manager on ProLiant sample configuration:

h18022.www1.hp.com/products/software/linux/mailmsg/mailstream.html

Sendmail Integrated Mail Suite on ProLiant sample configuration:

h18022.www1.hp.com/products/software/linux/mailmsg/mailsuite.html

Microsoft Exchange Server:

Microsoft Exchange info: www.microsoft.com/exchange

Microsoft TechNet Exchange guide:

www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/default.asp

Microsoft Exchange Trial Version:

www.microsoft.com/exchange/evaluation/trial/default.asp

Microsoft Exchange Information on ActiveAnswers:

h71019.www7.hp.com/2366-6-100-225-1-00.htm

IBM/Lotus Domino:

IBM/Lotus Domino info: www.ibm.com/domino, or http://www.lotus.com/products/r5web.nsf/webhome/nr5serverhp-new.

IBM/Lotus Domino v6 documentation:

www-10.lotus.com/ldd/notesua.nsf/ddaf2e7f76d2cfbf8525674b00508d2b/2f6cd8057c3602bf85256b5800681d38?OpenDocument

IBM/Lotus Domino information on ActiveAnswers:

h71019.www7.hp.com/281-6-100-225-1-00.htm

Novell GroupWise:

Novell GroupWise information: www.novell.com/groupwise

Novell GroupWise system requirements:

www.novell.com/products/groupwise/sysreqs.html

Novell GroupWise information on ActiveAnswers:

h71019.www7.hp.com/2611-6-100-225-1-00.htm

Novell GroupWise configuration:

www.novell.com/documentation/lg/gw6/index.html

Copy of IDC Report on groupware market:

www.microsoft.com/exchange/evaluation/compare/IDCICEReport/27600.htm