Sun Internet Mail Server^{TM}

Enabling the service-driven network, Sun Internet Mail Server software offers large enterprises and Internet Service Providers a reliable, manageable, and cost-effective Internet mail solution. With its wide ranging end-user access solutions, the power of Sun Internet Mail Server is readily available -- even to users who do not have e-mail client software.

Service - Driven Network

A service-driven network provides a dynamic and responsive network tuned for constant, consistent delivery of information services to networked users -- a network that enables companies and their customers to do business better, faster, and cheaper. This is the type of network achievable through the use of Sun software and systems products.

Organizations today require a dependable, cost-effective messaging system. Based on Internet standards, Sun Internet Mail Server software provides a highly scalable and complete messaging server solution that can be used effectively by enterprises or Internet Service Provider (ISP) operations. By enabling the deployment of a high-performance and reliable mail system, Sun Internet Mail Server delivers key information services within a service-driven network.

This white paper discusses the technical features of the Sun Internet Mail Server solution.

Better Quality of Service

Sun Internet Mail Server software is designed and built for business-critical use. The client/server design and committed message transport of Sun Internet Mail Server, combined with the proven reliability of Solaris Operating Environment software, delivers a truly robust mail system.

Designed on Internet Standards

Sun Internet Mail Server software is built on native Internet technology, so you can maintain a single architecture inside your organization and outside -- even when collaborating with your customers and partners. Plus, you aren't locked into a proprietary system. All key components of Sun Internet Mail Server are based on proven, open Internet standards such as:

- LDAP - Access to enterprise directory information, enabling an accurate, secure messaging system
- ESMTP - Extended messaging transport protocol for faster delivery and message status
- MIME - Message format definition enabling seamless exchange of messages
- HTML - Formatting language for providing Web browser access
- IMAP4 - Message access protocol delivering superior disconnected/remote user functionality
- POP3 - Established client protocol for compatibility with today's e-mail applications
- TCP/IP - Proven, worldwide networking protocol
- NOTARY - Defines message-status capabilities and delivery notification

Dependable

Sun Internet Mail Server software offers a number of features and capabilities to enable superior reliability. Sun Internet Mail Server provides maximum reliability, raising productivity while simultaneously reducing both administrative and opportunity costs. In version 3.5, that dependability is further enhanced with the addition of high availability.

Sun Internet Mail Server uses committed transactions at all interfaces to prevent lost or corrupted mail messages. The message store is built around a custom-designed database that employs a write-once data store and two-level index to achieve excellent performance and data integrity.

High Availability

Sun Internet Mail Server provides a high availability option in version 3.5. This option enables users to be serviced by a secondary Sun Internet Mail Server system if the primary system were to be taken offline for maintenance or other reasons.

Secure

Sun Internet Mail Server software offers secure connections for client and administrative sessions through its Secure Sockets Layer (SSL) support. This enables all communication between clients and the servers to take place inside an encrypted session. Furthermore, IPSec support provides secure server-to-server and client-to-server communication.

Today, one of the primary threats to messaging systems is an Unsolicited Bulk E-mail (UBE) attack, commonly referred to as spam. Sun Internet Mail Server software delivers improved capabilities in version 3.5 for dealing with UBE, including anti-relay features. Relaying through another server is the primary method for UBE attackers to target a site under a false identity. Sun Internet Mail Server enables administrators to easily set up anti-UBE rules by designating source address, destination address, source IP address, and the action that is desired. Anti-UBE rules help you to protect your organization from UBE attacks.

For enhanced security, Sun Internet Mail Server software can be integrated with Entrust/PKI to provide secure messaging through client-based S/MIME. With this integration, user security attributes such as X.509 certificates are stored in the directory used by Sun Internet Mail Server.

A messaging proxy server, a new option in version 3.5, can also be implemented to augment data security. A proxy server placed on the firewall with the actual messaging server behind it prevents attacks on the valuable information contained on the messaging server

Lowers Total Cost of Ownership

The Sun Internet Mail Server solution offers operating efficiencies in virtually all aspects of the messaging system, resulting in lower total operating costs. There is less hardware to buy and maintain per user, and less service downtime.

Sun Internet Mail Server works with a wide range of client solutions. Sun Messaging Connectivity Services helps you protect your existing investment.

Performance & Scalability

Sun Internet Mail Server software can support thousands of concurrently active POP3 and IMAP4 users. In a test audited by Shiloh Consulting, an independent company, Sun Internet Mail Server successfully supported 120,000 concurrent active POP3 and IMAP4 users on a single Sun Enterprise 6000 server. This means that an ISP provisioning for a maximum of 10% active users can host more than 1,000,000 total mailboxes on a single server.

The unsurpassed vertical scalability of Sun Internet Mail Server is complemented by the addition of horizontal scalability in version 3.5. This is accomplished through the use of a messaging proxy

option. A simple messaging server proxy implementation provides the ability to expand the capacity of a Sun Internet Mail Server environment by adding more servers. With proxies doing the work of routing the protocol traffic to and from the appropriate message store server, clients need only point to a single host name that provides access to their mail. This allows capacity to be added without any burden or reconfiguration on the clients.

Support for a Wide Range of Clients

Sun Internet Mail Server software features a single message store for POP3, IMAP4, and OpenWindows Mailtool environments, which enables you to have a single mail server for PC, UNIX, and Macintosh environments. Sun Internet Mail Server is tested with some of the most popular Internet mail clients such as Netscape Messenger, Microsoft Outlook Express, Qualcomm's Eudora Pro, CommTouch Software's Pronto E-Mail, and NetManage's Z-Mail.

If you have existing investment in non-Internet-standards-based clients such as Microsoft Windows Messaging Inbox or Microsoft Outlook, Sun Internet Mail Server software delivers tools to protect your investment. Version 3.5 contains MAPI service providers for IMAP and LDAP that give these clients access to the power of Sun Internet Mail Server.

Sun Internet Mail Server 3.5 software also features Sun Web Access software, which enables access of server-based e-mail, calendar, and directory information by any standard Web browser. It makes it possible for users to stay in touch anytime, anywhere

Manageability

Sun Internet Mail Server software features Java technology-based browser administration, which facilitates remote administration and decreases the need for on-site operators in remote locations. Administration tools are not only available through the administrative client but also through command-line utilities. This is a key requirement for Internet Service Providers. For example, message store quotas can be set for users in the administrative interface. To complement that, the administrator can use the quota notification utility to inform users that their mailbox has exceeded a set percentage of their mailbox quota

Architecture Details

Sun Internet Mail Server software is an extensible framework of cooperative modules that create an enterprise-wide, open standards-based, scalable electronic message-handling system. A message-handling system is the combination of message user and transfer agents, message stores, and access units that together provide electronic mail.

- Administration Services. The administration services of Sun Internet Mail Server software provide GUI-based configuration and monitoring. Sun Internet Mail Server is based Java technology.
- Message Access and Store. The message access and message store provides a repository of user messages as well as the means to retrieve and process those messages. The primary message store for Sun Internet Mail Server is the Sun Message Store, supporting both the Internet Message Access Protocol version 4 (IMAP4) and the less flexible but widely implemented Post Office Protocol version 3 (POP3). The mail server also retains support for the Solaris Mailbox Format Store to ease migration for sites with an installed base of clients using the traditional Berkeley- or UNIX V7-format mailbox, commonly referred to as /var/mail.

- Internet Message Transfer. The Internet Message Transfer Agent (IMTA) is responsible for the routing, transfer, and delivery of Internet mail messages. Sun Internet Mail Server software includes a fast, scalable, and flexible IMTA. This replaces the Sendmail utility bundled with most UNIX systems and used in Sun Internet Mail Server 2.0.
- Sun Directory Services. The directory is the central repository for meta-information: user profiles, distribution lists, and other system resources. Sun Internet Mail Server is bundled with a dedicated Lightweight Directory Access Protocol (LDAP) directory service.
- Sun Messaging Connectivity Services. Messaging software provides connectivity to proprietary message transfer systems, including the "LAN Mail" systems Lotus cc:Mail and Microsoft Mail, and the mainframe-base IBM OfficeVision (PROFS).

Administration

There are two means of administering Sun Internet Mail Server software. The Administration Console provides a GUI through which to manage the components. Alternatively, command-line utilities allow full configuration and management of the server. The Administration Console of Sun Internet Mail Server software leverages Java technology and enables maintenance, monitoring, and troubleshooting of the core Sun Internet Mail Server components. In addition, it provides access to fine-tune the default configurations of the various components and their interaction within the mail server.

The administrative services provided with the Sun Internet Mail Server product are composed of the following elements:

- Administration Console
- Administration Server
- Sun Internet Mail Server components

Sun Internet Mail Server Administration

The Sun Internet Mail Server product can be administered from the same machine that all the server components are installed on or, if desired, remotely from any machine on the network. The Administration Console provides the graphical user interface (GUI) that enables all configuration and management of the Sun Internet Mail Server components.

The Administration Server contains two major elements: a HyperText Transfer Protocol (HTTP) server and managed objects. The HTTP server residing on the Administration Server provides startup capabilities for certain Java elements. A HyperText Markup Language (HTML) file causes an initial applet and managed objects to be loaded from the Administration Server to the browser. (A managed object is a collection of configurable attributes; for example, a collection of attributes for the directory service.) After the initial applet takes control, it uses its managed object interfaces to communicate with the Administration Server.

The administration applet contains interfaces to the managed objects that reside in the Administration Server. The Administration Server interfaces with the directory access object using the Lightweight Directory Access Protocol (LDAP) and allows for provisioning of user and group attributes stored in the directory server. Each of the other server components communicates with the Administration Server using that component's native format, providing efficient communication and full access to the component features.

Sun Message Store

The Sun Message Store in the Sun Internet Mail Server software is a dedicated data store for the delivery, retrieval, and manipulation of Internet mail messages. This message store works with the IMAP4 and POP3 client access servers that ship with Sun Internet Mail Server to provide flexible and easy access to messaging. It saves any message that conforms to RFC 822 specifications, and recognizes the Multipurpose Internet Mail Extensions (MIME) content format.

The Sun Message Store is organized as a set of folders and user mailboxes. The mailbox is a container for messages. Each user has an Inbox where new mail arrives, and can have one or more folders where mail can be stored. Folders may contain other folders or mailboxes, and may be arranged in a hierarchical tree. Mailboxes owned by an individual user are private folders. In addition to a user owning a folder or a mailbox, a common user or group can share the ownership of a folder or mailbox. For example, the widget design team of the Acme Corporation, collectively known by the e-mail address widget-design@acme.com, can own a folder. A shared mailbox can be private or public.

A notable feature of the Sun Message Store is that it maintains only one copy of each message. If the Sun Message Store receives a message addressed to multiple users or a group or distribution list, it adds a reference to the message in each user's Inbox rather than having a copy of the message in each user's Inbox, thereby saving disk space. The individual message status (new, unread, replied to, deleted, etc.) is maintained per Inbox.

Sun Internet Mail Server software also supports the traditional Berkeley- or UNIX V7-format mailbox, commonly referred to as /var/mail. A site can implement both the Sun Message Store and /var/mail. Mail users can access both the Sun Message Store and /var/mail using the Internet Message Access Protocol version 4 (IMAP4) or the Post Office Protocol version 3 (POP3)

Internet Message Transfer Agent

The Internet Message Transfer Agent (IMTA) routes, transfers, and delivers Internet mail messages for the Sun Internet Mail Server product. The IMTA performs all of its operations on a set of channels. A channel is an interface with another Sun Internet Mail Server component, mail system, or mail user agent. There are two types of configurable channels: the inbound channels and the outbound channels.

An outbound channel is an interface between the IMTA and another Sun Internet Mail Server component (i.e., the Sun Message Store) or another component outside of the server (for example, the Internet or a local mail client). The IMTA delivers messages to other components over the outbound channel. Messages are likewise received over the inbound channels.

Each channel consists of up to two channel programs and an outgoing message queue for storing messages that are destined to be sent to one or more of the interfaces associated with the channel. Channel programs perform two functions:

- They transmit messages to other interfaces, deleting them from their queue after they are sent
- They accept messages from other interfaces, placing them or enqueueing them into channel queues

These external channels are configurable from the Administration Console providing powerful management of the mail system. Through channel configuration administrators can set a variety of parameters to control how messages are handled. This includes performance tuning as well as reporting aspects of the system. For example, multiple channels may be defined to segment traffic by groups or departments, message size limits may be defined to limit traffic, and delivery status notification rules may be defined according to the needs of the business. Diagnostic attributes are also a configurable.

Internet Message Transfer Agent -- Directory Cache

The IMTA needs to access the user and group or distribution list entries stored in the directory service for each message that it processes. Rather than querying the directory service each time it processes a message, the IMTA employs a cache of the directory information. It is this internally stored snapshot of the directory information that it accesses. This approach enhances the IMTA operation in the following ways:

- Improved Performance - Performing a directory query for each recipient of each message is time-consuming. It puts a large load on the directory server and may slow the mail server. The directory cache enables rapid processing.
- Streamlined Data Formatting - The information stored in the directory service is not always in the format needed by the IMTA. When creating the cache, the IMTA reformats the directory information.

Since the directory information stored in the directory service is continuously updated, the IMTA directory cache must be periodically synchronized with the current information in the directory service. For efficiency and flexibility, two types of synchronization are supported:

- Full Synchronization - The existing cache is rebuilt and then completely replaced with the current user and group entries from the directory service. After the synchronization occurs, the IMTA configuration file is rebuilt and the IMTA will automatically restart.
- Incremental Synchronization - The existing cache is updated with new user and group entries that were created or modified since the last full or incremental synchronization. Deleted users and groups are not updated during an incremental synchronization. The IMTA does not need to be restarted.

Since the IMTA does not need to be restarted with an incremental synchronization, there is little effect on the mail service availability. However, since deletions are not made until a full synchronization, messages to deleted users will continue to be processed

Sun Directory Services

Sun Internet Mail Server software is bundled with Sun Directory Services - a dedicated Lightweight Directory Access Protocol (LDAP) directory service. Sun Directory Services provides the central repository for meta-information: user profiles, distribution lists, and other system resources. This directory supports the storage of information according to a directory information tree (DIT). The DIT is a hierarchical structure that resembles a tree with one major branch at the top and many branches and sub-branches below. The arrangement of the tree is flexible, allowing administrators to decided how to best deploy the service for their organization. For some, it may be best to arrange the tree according the actual business organizational structure or geographic structure. For others, a one-to-one mapping to DNS layers may be best.

The DIT also provides the flexibility to support a wide range of administration scenarios, and can be administered in either a centralized or distributed manner. Centralized administration can be implemented where one authority manages the entire DIT. This type of administration is usually used in scenarios where the entire DIT resides on one mail server.

Distributed administration can also be implemented with multiple authorities managing the DIT. This type of administration is usually implemented when the DIT is divided into portions - or subtrees - and the subtrees reside on different mail servers. When the DIT is large in size or when mail servers are geographically dispersed, it may be beneficial to delegate management of portions of the DIT.

Typically, in this scenario, an authority is assigned to manage each subtree of the DIT. Sun Internet Mail Server software allows for one authority to manage multiple subtrees, however for security reasons, an authority can make changes only to the subtree of the DIT that he or she owns

Directory Replication

The directory service also supports replication, allowing for a variety of configurations to provide redundancy and efficiency. By enabling all or part of the DIT to be replicated from one directory server to one or more other directory servers, the most flexible configuration capabilities are provided.

- The directory information is more accessible since it is replicated on multiple servers rather than a single directory server.
- The directory information is cached on a local directory server, saving the effort of accessing the information from a remote directory server and thereby enhancing performance.
- Depending on the actual configuration, requests generated by mail clients may be processed faster by multiple directory servers rather than by one centralized directory server.

Messaging Connectivity

Sun Messaging Connectivity Services connects the Sun Internet Mail Server product to proprietary mail transfer systems, and supports integration of users from those systems to native Internet standards-based messaging. Specifically, Sun Messaging Connectivity Services provides batch-mode connectivity to:

- Lotus cc:Mail
- Microsoft Mail
- IBM's mainframe-base OfficeVision (PROFS)

Sun Messaging Connectivity Services is composed of a back-end server and messaging front-end systems that talk to the proprietary mail clients. It utilizes the channel concepts within the IMTA to perform the message format conversions and coordinate the flow of messages between the Sun Internet Mail Server system and other proprietary mail systems.

Channels

A channel is an interface with another Sun Internet Mail Server 3.5 component, mail system, or mail user agent. The actual hardware connection, software transport, or both may vary widely from one channel to the next. As discussed earlier (see Internet Message Transfer Agent section, page 10), the IMTA has two types of configurable external channels: one for inbound messages and one for outbound messages. In addition, there is a third type of channel in the IMTA -- an internal channel -- used for internally processing a message.

When connecting with a proprietary mail system, an inbound channel converts the inbound message to the canonical format and then sends the message to the router. The router reads the canonical address to determine the destination and passes the message to the channel associated with the recipient's local mail network. An outbound message is then converted to the outbound channel's message format and passed to the outbound channel's transport for delivery into the client mail agents.

Some of the default channels provided with Sun Internet Mail Server software are:

- SMTP Channel: TCP/IP-based message delivery and receipt
- Pipe Channel: Used for alternative message delivery programs; allows delivery of messages to programs such as a mail sorter rather than directly to a users inbox
- Local Channel: Delivers mail to /var/mail; provides for compatibility with older UNIX mail clients
- Reprocessing Channel: Useful for messages that are resubmitted Defragmentation Channel: Reassembles partial messages into the original complete message
- Conversion Channel: Performs body part by body part conversion on messages; useful for rewriting addresses or re-formatting messages

Transports

Transports are background programs that transfer messages between networks. Some channels have a client component that interfaces between the server and the local computing environment. Others, such as SMTP/MIME, act as full peer message transfer agents (MTAs). Each transport program supports multiple channels.

NJE Transport The NJE Transport provides a method of transferring messages between IMTA, Sun Messaging Connectivity Services, and mail systems running the NJE networking protocols, such as PROFS/OfficeVision. The NJE Transport treats the host as a virtual NJE node, making the addressing nomenclature transparent.

SPX Transport The SPX Transport provides an Ethernet-based method for transferring messages with a PC-based SPX client program. This type of transport communicates directly with the Microsoft Mail client for message transfer.

File Sharing Transport The File Sharing Transport moves messages between the UNIX operating system and the PC running a client through a shared file system available to both platforms. When a channel is configured to use File Sharing Transport, the shared directory to use for the

file exchange must be specified.

High Scalability/High Performance

Sun Internet Mail Server software can support thousands of concurrently active POP3 and IMAP4 users. In a test audited by Shiloh Consulting, Sun Internet Mail Server successfully supported 120,000 concurrent active POP3 and IMAP4 users on a single Sun Enterprise 6000 server. This means that an ISP provisioning for a maximum of 10% active users can host more than 1,000,000 total mailboxes on a single server. Maximum performance is achieved by multithreading all core components, taking advantage of state-of-the-art multiprocessor hardware platforms, and optimizing Solaris I/O. Sun Internet Mail Server seamlessly gains in performance proportional to the scales of the Sun server platform.

Ultimately, most mail systems will support Internet standards. But simply supporting those standards will not mean that they can deliver the same performance and cost of ownership to customers. How the implementation is carried out is critical to the performance delivered. For example, unlike some other mail systems, Sun Internet Mail Server retains duplicate copies of a message while processing it to ensure it is not damaged in handling.

Sun has been delivering Internet standards-based mail for many years. Some vendors have added "bolt-on" translators or gateways to be able to handle Internet mail. How each component in the mail system (Message Transfer Agent, message store, and directory service) is implemented and how they are all integrated together determines how well the entire mail system will perform. Some examples of the superior integration of the Sun Internet Mail Server design follow.

Intelligent Virtual Memory Management

In some mail system implementations, virtual memory requirements may actually equal mailbox size. This can severely limit the number of users that can be supported. In addition, with mailbox size varying significantly, capacity may be poorly optimized. Sun understands these issues and has addressed them. In the Sun Internet Mail Server product, the virtual memory usage has be reduced to a function of the number of users, number of messages, and number of active connections. Unlike other implementations, the size of the mailbox or size of messages in the mailbox is not a factor.

Since the sizing requirement in Sun's design is smaller -- based on the number of messages and not the message size -- up to ten times the number of users can be placed on the same system versus other solutions. Additionally, with the corresponding lower virtual memory usage, user response times are improved.

Advanced Message Store Design

The design of the Sun Message Store provides unique performance and scalability improvements over other messaging systems. Older mail systems have utilized a single file store for each user or a single file per message. In the single file per user case, the entire mailbox must be re-written for changes such as when a single piece of mail is deleted or when a message status is changed. For example, the traditional UNIX /var/mail system works in this manner.

Other message store designs use a model of one directory for all users and every piece of mail is a file. This is an improvement, however there remain a number of limitations including the fixed limit of 32,000 users due to UNIX file system restrictions. In addition, it is difficult to search a

directory with 32,000 entries in it. The design used in the Sun Internet Mail Server product introduces the use of a hash table and structure with no more than 200 users per directory.

Super-Threaded Design

In the Solaris Operating Environment there are multiple Solaris threads available per heavyweight process, and thread management is in the user space. Sun Internet Mail Server software can support 200 IMAP4 or POP3 connections per lightweight process. The server's threads are designed to do very little processing and thus consume very little CPU. For example, with Sun Internet Mail Server product, I/O is controlled through a single thread. Other systems may end up utilizing only one thread per lightweight process, resulting in lower overall system performance and lower user capacity per server.

Products that run on Windows NT are significantly more limited. Windows NT has a fixed limit of one thread per lightweight process. A thread and a lightweight process are the same thing as far as system resource utilization is concerned, and all thread management happens in kernel space. This requires more memory usage and more context switches for the same amount of mail processing.

Threading is not specific to the hardware architecture as it works on Intel x86 and SPARCTM systems. In addition, Sun Internet Mail Server utilizes threading throughout the system. The Message Transfer Agent has multithreaded connectivity to the message store and the queuing model takes advantage of the threading as well. The message store and directory services also take advantage of Solaris threads.

Smart Indexing

Indexing can improve message retrieval and user capacity under load. For each message, Sun uses two (2) levels of indexing. As discussed earlier, some message store designs use a single file-per-user (with no indexing) or a single, file-per-message approach. The latter implementations may use the UNIX file system as a first level of index. The two levels of indexing allows segmentation of status changes that can be rapidly updated and the ability to keep just one copy of the mail message for multiple recipients. Other mail systems such as the traditional UNIX /var/mail system keep X copies for X recipients. The Sun Internet Mail Server design leads to much better disk utilization.

Sun's two (2) levels of indexing per message enables excellent search and retrieval performance and scalability as more messages or more users are added. With Sun Internet Mail Server software, messages are pre-parsed (upon receipt) and the results are kept in an index. With Sun Internet Mail Server, instead of searching an entire mailbox including message bodies, only the index need be searched.

Finally, the superior organization enabled by indexing means potentially higher performance. Since each index and data can be kept in separate directories, it is possible to put different directories on different spindles and optimize disk I/O. Others systems tend to keep indexes close to files. Being able to get these on different spindles and cut down the disk seeks is inherently faster.

Sensible Message Parsing (IMAP4 Only)

All POP mail designs assume messages are downloaded to the client. Only IMAP systems can take advantage of this feature. Most implementations do parsing on demand. Each time a user

opens a message, the message is parsed. Alternatively, some mail systems do parsing when a folder is opened. These systems will parse all the messages when the folder is opened and will keep the parsing results in virtual memory. However, when the user exits the results disappear. Next time the folder is opened, all the messages will have to be parsed once again.

The Sun Internet Mail Server product performs a pre-parsing operation. Messages are parsed as they arrive and the results stored until the messages are deleted. This means that the load due to parsing is evenly distributed and the overall peak loads when users are performing other functions is lower. Tuning is also available since this function can be turned off for POP users.

Fast Message Delete

Expunge operations -- the deletion of messages -- is time consuming for many mail systems. If the message store is designed with a single file per user, deleting messages means a rewrite of the whole file, that is rewriting every message in the Inbox into a single file. The operation's activity is proportional to size of mailbox.

If the mail system uses a one file-per-message design, then deleting messages means deleting individual message files. This is more efficient than rewriting the entire list of messages kept, however it requires synchronous directory operation for every delete. This synchronous I/O can be taxing, particularly with many simultaneous users performing other functions. Since these operations are run per file, each must be done one at a time. This means that 100 deletions requires 100 directory I/O operations.

Sun uses a one index-per-user message store design and a centralized delete operation. To expunge a message means a rewrite of an index file. This is the same as the previous delete operation for a single file, however the single file in this case is small (perhaps 48 bytes) and dependent on message count not message size (48K at 1000 messages). The index is all that changes at the time the user deletes a message. The actual file deletion occurs at a non-peak time in an aggregated fashion. With this approach, deletions occur quickly for each user, and server computation and synchronous I/O is minimized during peak usage.

Configuration and Deployment Flexibility

Sun Internet Mail Server software provides a number of significant configuration capabilities that allow it to provide exceptional deployment flexibility. Using hardened Internet standards intelligently, Sun Internet Mail Server is capable of reliably supporting most mail deployment scenarios with high performance and broad functionality. In particular, several features of the Sun Internet Mail Server product expand its capabilities beyond those found on other systems, including:

- Web Access to Mail
- Anti-UBE (Anti-Spamming)
- Proxy Message Access Configurations
- Proxy Server Models
- Using the Sun Internet Mail Server with SSL

Web Access to Mail

Sun Web Access is fully integrated browser-based software that provides access to Sun Internet

Mail Server 3.5 e-mail, Sun Directory Services, and to the SunTM Calendar Server. Sun Web Access is integrated with the Sun Internet Mail Server 3.5 server system and centrally administered, so installation involves little more than providing end users with a URL to the Sun Web Access server. End users can then open an Internet browser, enter the URL, and launch Sun Web Access.

End users can invoke and run Sun Web Access from any Internet browser that is capable of displaying HTML 3.2-compliant documents with frames running on any platform, including Microsoft Windows, Macintosh, OS/2, and DOS desktops. Sun Web Access uses Java Web Server 1.1 servlet technology.

Sun Web Access integrates core Internet-based message services such as:

- MailView - An IMAP4/SMTP mail service
- CalendarView - A versatile personal and workgroup scheduling tool
- NameView - An enterprise or department-wide name directory

Sun Web Access is extensible for push-button links to site -- or department-wide applications, and can be secured by incorporating the Secure Socket Layer (SSL). It also enables users to view calendars managed by the CDE calendaring server (rpc.cmsd) running on Solaris 2.5.1, 2.6, and compatible systems. A CDE calendar needs to be created before the user can utilize Calendar in Sun Web Access.

Anti-UBE (Anti-Spamming)

Anti-Relay
The message access and relay restriction features of the Sun Internet Mail Server allow you to restrict messages from passing through Sun Internet Mail Server software based on source and destination e-mail address, IP address, and domain. This feature provides several types of functionality:

- Limits UBE by blocking unwanted mail delivery
- Limits UBE by not relaying (sending mail from one domain to another) unwanted mail
- Restricts e-mail usage to internal users

Some other mail systems may also provide the ability to purge unwanted messages, however they will store messages first and then examine them to determine appropriate action. With a large number of messages, as in a denial of service attack, this can be costly and may cause the system to go down. Through its flexible architecture, the Sun Internet Mail Server product is able to examine and discard unwanted messages upon receipt before they are processed by the server or put in the message store. Specifically, Sun Internet Mail Server allows e-mail to be blocked by the following specified elements:

- By source or destination domain
- By source client IP address
- By destination server IP address
- By source or destination e-mail address

Through these attributes, Sun Internet Mail Server software allows specifically known addresses of abuse to be blocked. It also allows only those messages to or from specified addresses to be processed. The range of capability in the server provides significant flexibility to ensuring that unsolicited e-mail does not affect the performance of the system.

Controlling Port and E-Mail Access

An individual can intentionally or inadvertently overwhelm your mail server by flooding it with messages. This type of act is called a denial of service attack. If a denial of service attack is perpetrated against the mail server, there may be either a substantial impact to the throughput of the mail server or the mail server will become overloaded and nonfunctional.

Sun Internet Mail Server software provides three features that enable administrators to minimize the possibility of a denial of service attack:

- Port Access - Enables you to specify which incoming Simple Mail Transfer Protocol (SMTP) connections are accepted or denied based on IP addresses and port numbers
- E-Mail Access Restrictions - Enables you to specify which incoming messages are accepted or denied based on channel names and e-mail addresses
- Message Size Limits - Enables you impose a limit at which a message is deemed too large and rejected by a channel

Proxy Message Access Configurations

Normally, the Sun Internet Mail Server product acts as both a mail delivery server and a message access server. That is, the server can handle requests to send mail or to retrieve mail from mailboxes. It is also possible, however, to configure Sun Internet Mail Server as a proxy message access server.

A proxy mail access server looks exactly like a real message access server, however it is only a front end to a real server. The proxy accepts client POP/IMAP requests for mailbox access, authenticates the requestor's password, then forwards the request to the appropriate mail server (i.e., the server containing the desired mailbox). Once the authentication and connection to the real mail server has been made, the proxy acts as a simple pipe between the client and the real mail server, forwarding whatever one sends to the other until either the client or the server closes the connection.

Although a proxy server does not allow for message storage, from the client's point of view the proxy acts just like a regular mail server. Because the proxy communicates with the real mail server using POP/IMAP, from the real mail server's point of view the proxy appears as another mail client.

The Sun Internet Mail Server message access proxies have two configurations: a pure proxy,

which acts only as a proxy for the Sun Internet Mail Server mail servers; and a message access proxy/message access server, which can act as a proxy for some mail addresses and as a full mail server for local addresses.

Proxy Server Models

Proxy servers are useful for a number of applications. How you deploy proxy servers depends on the specific configuration of your e-mail system and what your goals are. This section describes three possible scenarios and models where proxy servers could be used.

Proxy Servers for Horizontal Scalability

Horizontal Scalability is the ability to expand the capacity of a Sun Internet Mail Server environment by adding more servers. Message access proxy servers make horizontal scalability possible by having clients point to a single host name that provides access to their mail. Proxies do the work of routing the protocol traffic to and from the appropriate message store server. Since proxies allow clients to access their mail folders through a host name which is independent of the actual message store host name, capacity can be added without any burden or reconfiguration on the clients. (For example, having to reconfigure the message access server on each client.)

In implementations requiring multiple server systems, without proxy servers each user would have to specify their server host name to retrieve mail. By using proxy servers with the Sun Internet Mail Server, messages can be accessed through one virtual mail server, while any number of actual mail servers perform actual message storage and retrieval.

By offering only one single virtual mail server, ISPs or corporate administrators can add additional mailbox capacity by simply adding more servers behind the proxies.

Users log in to the system using the domain name mail.isp.net. For an enterprise deployment, this might be mail.enterprise.com. Mail requests are routed through the system and sent to a proxy server via round-robin DNS (DNS that can return more than one IP address in round-robin fashion to distribute load among multiple proxy servers). The message access proxy authenticates the user through a replicated LDAP directory, then sends the request to the appropriate message access server. Additional capacity is achieved by adding more message access servers behind the proxies.

This deployment enables easy expansion of capacity, and by virtue of round-robin DNS, allows mail access proxies to be treated as field replaceable units. If mail.isp.net (or mail.enterprise.com) needs to expand message store capacity to accommodate new customers they can do so either by expanding the capacity of an existing message store server (by adding system resources, or they can add a new message store server). In either case, clients will not be required to change their mail server hostname setting.

Proxy Servers for Internet Mail Access

A company that protects its network behind a firewall could, by using a proxy server, allow employees to access their e-mail outside the firewall through the global Internet instead of maintaining a private modem-pool to connect to their intranet directly.

Internet Mail Access, an Internet mail client accesses his/her mail through a proxy server on the firewall via a secure IMAP connection. The proxy authenticates the user, then forwards mail store requests to the Sun Internet Mail Server system. The server then sends message data to the

proxy, which in turn forwards it to the mail client

Using the Sun Internet Mail Server with SSL

SSL is an open, non-proprietary security protocol. It has been submitted to the W3 Consortium (W3C) Working Group on Security for consideration as a standard security approach for World Wide Web browser and servers on the Internet. SSL provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection between a client and a server, or a server and a server.

Using SSL with Sun Internet Mail Server software ensures security between a mail client and the server by encrypting the session in which e-mail content is transferred between Sun Internet Mail Server and the e-mail client. Since SSL provides encryption at the level of the network connection, different ports are used for secure and non-secure communications. Port 993 is the default port for secure IMAP4 connections; port 995 is the default port for secure POP3 connections.

Deploying a secure mail solution with the Sun Internet Mail Server product is made easier by the interoperability of the server with key management products such as available from Entrust. Working together, the Sun Internet Mail Server 3.5, Sun Directory Services 3.1 and the Entrust/PKI form a secure messaging solution using client-based S/MIME. Enterprise IT professionals who wish to take advantage of the high performance and other features offered by Sun Internet Mail Server 3.5 may wish to integrate it into the Entrust infrastructure. Both products rely on Sun Directory Services as their LDAP server, so integration between the two can be done fairly easily. Sun Professional Services is available to help with this effort.

Once integration is complete users can utilize an Entrust/Client and the Entrust-Ready Netscape Communicator to:

- Encrypt and digitally sign files
- Decrypt encrypted files and verify digital signatures on signed files
- Securely delete files

Entrust uses an LDAP compliant directory service (such as Sun Directory Services) that contains the entries of each person in the organization. These persons could also be Sun Internet Mail Server 3.5 "emailPerson" entries that have Entrust attribute information appended to them. The directory also holds certificate revocation lists (CRLs). These are lists of certificates that have been revoked. The Entrust infrastructure requires the LDAP v3 protocol, therefore only version 3.1 of Sun Directory Services may be used.

Both the Entrust/Client and Entrust-Ready Netscape client communicate directly to the directory. Whenever a user sends a message to a group of recipients, Netscape contacts the directory to get each recipient's public-key certificates for encryption.

Sun Internet Mail Server High Availability

A major advantage of the Sun Internet Mail Server product over competitors is its superior scalability, which enables populating large number of users on just one server. Although this

provides excellent price versus performance advantages, it could result in a single point of failure, where one failing machine could interrupt e-mail access for an entire user community.

To ensure reliability, Sun Internet Mail Server 3.5 can be installed on a Sun Enterprise cluster by using the Sun Cluster 2.1 software. This capability provides automatic fail over when a system shutdown or failure occurs.

Sun Internet Mail Server Asymmetric HA Configuration

Each node in the cluster is a complete Solaris system with its own private disk that contains the operating environment and the Sun Cluster software.

Asymmetric HA Configuration Since each node has at least one network interface connected to the public network, users can connect through this interface to read their mail messages. Each node has at least two additional private network interfaces that connect to corresponding private network interfaces on the other members of the cluster. These are used by the Sun Cluster software on each node for system status monitoring and cluster configuration data sharing. Only one pair of private network interfaces is in use at any given time; the other is a redundant interface to guard against there being a single point of failure.

Each node has a connection to the disk cluster that contains the message store, message queues, directory contents, configuration files, and Sun Internet Mail Server binaries. While both nodes are connected to the disk cluster continuously, the volumes in the disk cluster are mounted on only one of the nodes at any given time. Figures 4 and 5 show this disk cluster as a single logical volume. Sun Cluster also includes the Sun Enterprise Volume ManagerTM, based on the Veritas Volume Manager. This allows a logical volume to be mirrored across multiple physical volumes, providing uninterrupted service even if a physical disk fails.

Only one of the nodes in the cluster runs Sun Internet Mail Server software at any time. This represents an Asymmetric High Availability (HA) configuration. In this configuration, all the Sun Internet Mail Server binaries, configuration files, message queues, and message store reside on a shared disk. As a result, when a failover occurs, the disk is unmounted from the failing system and mounted on the surviving system.

Asymmetric HA Configuration After Failover The logical IP address is now configured on the public network interface of the other system. Users and mail agents on the public network always connect using the logical IP address. Thus, re-connecting after a failure automatically connects to the other system. A failover, will then, appear to be a very quick crash and re-boot of a single system.

Since the SMTP and POP protocols automatically connect, perform a transaction, and then disconnect, users and agents using those protocols may not even notice that a system failure has occurred. IMAP clients tend to connect and stay connected; when the failover occurs, most of them will pop up a dialog box to inform the user about the dropped connection and ask if the user would like to re-connect.

In the Sun Internet Mail Server Asymmetric HA configuration, the other node in the cluster is idle as far as Sun Internet Mail Server usage is concerned. This node, however, remains a fully-functional Solaris system and is available for other work as long as procedures to terminate or limit the other work after a failover are in place.

As long as the CPU speed and memory size of the two nodes in the cluster are alike (recommended) in this Asymmetric HA configuration, the performance does not suffer during a fail-over.

System Requirements
Mail server configurations can vary significantly depending on user requirements. Please check with your Sun consulting representative, consultant, or reseller for more details.

Server Requirements:

- Solaris 2.5.1 and 2.6 Operating Environment software on SPARCTM or
- Intel Pentium platforms 90 Mbytes of disk space for product installation 64 Mbytes of memory minimum; more for larger deployments

Client Requirements:

- For Sun Web Access software, an HTML v3.2 compliant Web browser For MAPI providers, Microsoft Windows Messaging Inbox or Microsoft Outlook

Standards Support

- Messaging and hosts: RFC 822, 1123
- Directory: ITU X.520, X.521, RFC 1274, 1781
- SMTP & ESMTP: RFC 821, 1652, 1869, 1870,1893
- LDAP: RFC 1777, 1778, 1779, 1798
- IMAP4: RFC 1730-3, 2060, 2061
- POP3: RFC 1939
- MIME: RFC: 2017, 2045-9
- NOTARY: RFC 1891-1894
- UUCP: RFC 976
- DNS: RFC 974, 1034, 1035
- Gateways: PC-WIN, PC-850 PC-437
- Character Sets: IA5, ISO 2022, JIS X 0201, 0208, JUNET, US ASCII, US LATIN, RFC 1345, 1468, 1502