MIRAPOINT®

Site Planning Guide

Release 4.0
December 2007
Part number 010-00543c

This manual supports Messaging Operating System (MOS) release 4.0.4 and later MOS releases until replaced by a newer edition.

Macintosh is a trademark of Apple Computer, Inc.

Windows, Outlook, Exchange, and Active Directory are trademarks of Microsoft Corporation.

Java and Solaris are trademarks of Sun Microsystems, Inc.

Linux is a registered trademark of Linus Torvalds.

All other trademarks are the property of their respective owners.

OTHER THAN ANY EXPRESS LIMITED WARRANTIES THAT MIRAPOINT PROVIDES TO YOU IN WRITING, MIRAPOINT AND MIRAPOINT'S LICENSORS PROVIDE THE SOFTWARE TO YOU “AS IS” AND EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MIRAPOINT'S LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE OR OTHER TORT), ARISING IN ANY WAY OUT OF YOUR USE OF THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF DAMAGES. Mirapoint's liability shall be as limited in the License Agreement.

MIRAPOINT SOFTWARE, INC. SOFTWARE LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT (“LICENSE”) CAREFULLY BEFORE DOWNLOADING OR OTHERWISE USING THE SOFTWARE. BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, YOU ARE NOT AUTHORIZED TO DOWNLOAD OR USE THIS SOFTWARE.

1. Scope. This License governs your use of any and all computer software, any printed or electronic documentation, or other code, whether on disk, in read only memory, or on any other media (collectively, the “Mirapoint Software”) provided to you as part of or with a Mirapoint Product.

2. License, not Sale, of Mirapoint Software. The Mirapoint Software is licensed, not sold, to you by MIRAPOINT SOFTWARE, INC. or its affiliate, if any (“Mirapoint”). YOU MAY OWN THE MEDIA ON WHICH THE MIRAPOINT SOFTWARE IS PROVIDED, BUT MIRAPOINT AND/OR MIRAPOINT’S LICENSOR(S) RETAIN TITLE TO THE MIRAPOINT SOFTWARE. The Mirapoint Software installed on the Mirapoint Product and any copies which this License authorizes you to make are subject to this License.

3. Permitted Uses. This License allows you to use the pre-installed Mirapoint Software exclusively on the Mirapoint Product on which the Mirapoint Software has been installed. With respect to Mirapoint Software [identified by Mirapoint as the “administrative application” that has not been pre-installed on the Mirapoint Product, this License allows you to copy, use and install such Mirapoint Software on one or more administrative workstations on which the Mirapoint Software is supported. You may make one copy of the Mirapoint Software in machine-readable form for backup purposes only, provided that such backup copy must include all copyright and other proprietary information and notices contained on the original.

4. Proprietary Rights; Restrictions on Use. You acknowledge and agree that the Mirapoint Software is copyrighted and contains materials that is protected by copyright, trademark, trade secret and other laws and international treaty provisions relating to proprietary rights. You may not remove, deface or obscure any of Mirapoint’s or its suppliers’ proprietary rights notices on or in the Mirapoint Software or on output generated by the Mirapoint Software. Except as permitted by applicable law and this License, you may not copy, decompile, reverse engineer, disassemble, modify, rent, lease, loan, distribute, assign, transfer, or create derivative works from the Mirapoint Software. Your rights under this License will terminate automatically without notice from Mirapoint if you fail to comply with any term(s) of this License. You acknowledge and agree that any unauthorized use, transfer, sublicensing or disclosure of the Mirapoint Software may cause irreparable injury to Mirapoint, and under such circumstances, Mirapoint shall be entitled to equitable relief, without posting bond or other security, including but not limited to, preliminary and permanent injunctive relief.

5. Disclaimer of Warranty on Mirapoint Software. You expressly acknowledge and agree that use of the Mirapoint Software is at your sole risk. Unless Mirapoint otherwise provides an express warranty with respect to the Mirapoint Software, the Mirapoint Software is provided “AS IS” and without warranty of any kind and Mirapoint and Mirapoint’s licensor(s) (for the purposes of provisions 5 and 6, Mirapoint and Mirapoint’s

licensor(s) shall be collectively referred to as "Mirapoint") EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN ADDITION, MIRAPOINT DOES NOT WARRANT THAT THE MIRAPOINT SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE MIRAPOINT SOFTWARE WILL RUN UNINTERRUPTED OR BE ERROR-FREE, OR THAT DEFECTS IN THE MIRAPOINT SOFTWARE WILL BE CORRECTED. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR OTHER DISCLAIMERS, SO THE ABOVE EXCLUSION OR DISCLAIMERS MAY NOT APPLY TO YOU.

6. Limitation of Liability. UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL MIRAPOINT BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS LICENSE. FURTHER, IN NO EVENT SHALL MIRAPOINT'S LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE, DATA OR PROFITS OR INTERRUPTION), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE OR OTHER TORT), ARISING IN ANY WAY OUT OF YOUR USE OF THE SOFTWARE OR THIS AGREEMENT, EVEN IF ADVISED OF THE POSSIBILITY OF DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Mirapoint's total liability to you for all damages exceed the amount paid for this License to the Mirapoint Software.

7. Government End Users. If the Mirapoint Software is supplied to the United States Government, the Mirapoint Software and any documentation are provided with RESTRICTED RIGHTS. The Mirapoint Software is classified as "commercial computer software" and the documentation is classified as "commercial computer software documentation" or "commercial items," pursuant to DFAR Section 227.7202 or FAR Section 12.212, as applicable. Any use, modification, reproduction, display or disclosure of the Mirapoint Software or any documentation by the United States Government shall be governed by the terms of this License.

8. Miscellaneous. This License will be governed by and construed in accordance with the laws of the State of California, U.S.A., without reference to its conflict of law principles. If a court of competent jurisdiction finds any provision of this License invalid or unenforceable, that provision will be amended to achieve as nearly as possible the same economic effect as the original provision and the remainder of this License will remain in full force. Failure of a party to enforce any provision of this License shall not waive such provision or of the right to enforce such provision. This License sets forth the entire agreement between the parties with respect to your use of the Mirapoint Software and supersedes all prior or contemporaneous representations or understandings regarding such subject matter. No modification or amendment of this License will be binding unless in writing and signed by an authorized representative of Mirapoint. You will not export, reexport, divert, transfer or disclose, directly or indirectly, the Mirapoint Software, Mirapoint Products or any technical information and materials supplied under this Agreement without complying strictly with the export control laws and all legal requirements in the relevant jurisdiction, including without limitation, obtaining the prior approval of the U.S. Department of Commerce.

Contents

List of Figures

List of Tables

Preface

Welcome to the *Mirapoint Site Planning Guide*. This book helps prepare IT managers and system administrators to deploy Mirapoint messaging solutions. This book introduces Mirapoint's messaging architecture, describes several common deployment scenarios, and gives a detailed overview of Mirapoint's security and message server features.

This book assumes that you are familiar with industry-standard networking terminology and have a general understanding of how Internet email messaging works. For an overview, see the Wikipedia email article at

http://en.wikipedia.org/wiki/Email.

Important terms are defined in the Glossary on page 79.

About Mirapoint Documentation

Documentation for all Mirapoint products is available through the Mirapoint Technical Library (MTL) on the Customer Support website:

http://support.mirapoint.com/secure/MTL/MTL

The MTL provides the Hardware and Software documentation for all supported Mirapoint releases and appliances, a Glossary, and the Support Knowledge Base. The Support site is accessible to all customers with a valid Support Contract. If you have a valid Support Contract but need a Support login ID, send an email to:

support-admin@mirapoint.com

Typographic Conventions

Table 1 on page 13 explains what different fonts in this book indicate.

Table 1 Typefaces Used in this Book

Typeface	How it is Used	Examples
Roman	Ordinary text	The server organizes folders hierarchically.
Bold	Definitions; also screen elements such as menus, commands, and option labels	A **folder** contains messages. Use the **Ldap Set** command to enable autoprovisioning.

Table 1 Typefaces Used in this Book (Continued)

Typeface	How it is Used	Examples
Italic	Emphasis; book titles	Add *at least two* DNS servers. See the *Administrator's Guide*.
`Typewriter`	Screen display; command names	`Enter your password:`
`Typewriter Bold`	Text you type exactly as shown	**`Smtp Set Smtpauth`**
`Typewriter Italic`	Markers for variables you provide	*`IP_address`*

Icon Conventions

Table 2 explains what the different icons in this book indicate.

Table 2 Icons Used in This Book

Icon	Indicates
	Important information.
	Best practices.

About this Book

This book provides information about Mirapoint's messaging architecture and deployment options for a Mirapoint appliance-based messaging solution, as well as a detailed overview of Mirapoint's security and messaging features:

- Chapter 1, Introduction to Mirapoint Solutions provides an overview of the Mirapoint messaging architecture.
- Chapter 2, Mirapoint Deployment Scenarios describes the most common deployment scenarios for Mirapoint appliance-based messaging solutions.
- Chapter 3, Planning for Deployment describes the deployment process, infrastructure requirements, and site preparation procedures for deploying Mirapoint appliances.
- Chapter 4, Security Features Overview describes the security features of a Mirapoint deployment.
- Chapter 5, Message Store Overview describes the messaging features of a Mirapoint deployment.

1 Introduction to Mirapoint Solutions

This chapter introduces the components of a secure messaging infrastructure and describes the Mirapoint messaging architecture.

Building a Secure Messaging Infrastructure

Mirapoint's email server and security appliances are the building blocks for a secure messaging infrastructure that intelligently serves, secures, and manages email. Mirapoint messaging solutions go beyond basic person-to-person email, addressing requirements for mobile access, group collaboration, and regulatory compliance, while providing unparalleled performance, reliability, and security.

- Mirapoint MailHurdle appliances block 50-80% of spam & email-borne viruses at the SMTP-layer before they enter the network, thereby conserving bandwidth, storage & administrator resources.
- Mirapoint RazorGate appliances block spam, protect against viruses and hacker attacks, and filter content for both inbound and outbound messages, as well as route and proxy.
- Mirapoint Message Server (MMS) appliances provide a comprehensive messaging platform that intelligently serves, secures, and manages messages with multi-mode client access. In addition to email services, Message Server also provides easy-to-use collaboration tools, including group calendaring, scheduling, and address book.
- Mirapoint Directory Server appliances form the backbone of the messaging network by providing unified user and system management. Directory Server simplifies the creation, use, and integration of LDAP directories as a common information database for all messaging and related applications.
- Mirapoint applications and APIs support desktop interfaces, mobile devices, and web-based access.

Figure 1 illustrates how the Mirapoint appliances work together to form a secure messaging infrastructure.

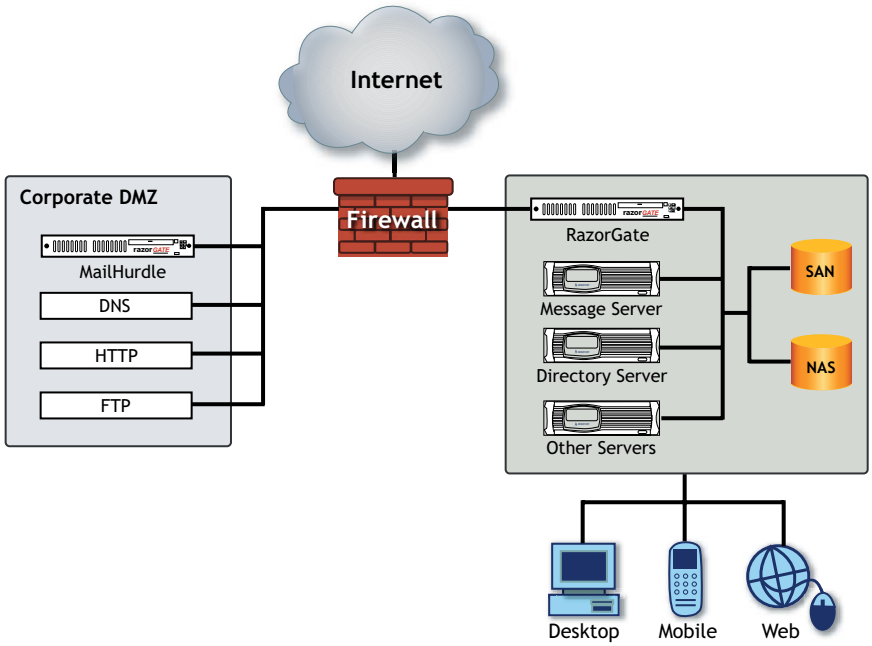

Figure 1 Secure Messaging Infrastructure

Mirapoint's flexible messaging architecture makes it easy to build a messaging infrastructure that not only meets your current demands but can easily be expanded to accommodate future growth.

Mirapoint Messaging Architecture

Mirapoint's messaging architecture consists of security and messaging functions that can be distributed across multiple RazorGate, Message Server, and Directory Server appliances to increase capacity and performance. Requests are transparently routed to the appropriate locations within the messaging network.

Figure 2 shows the security and messaging functions in Mirapoint's messaging architecture.

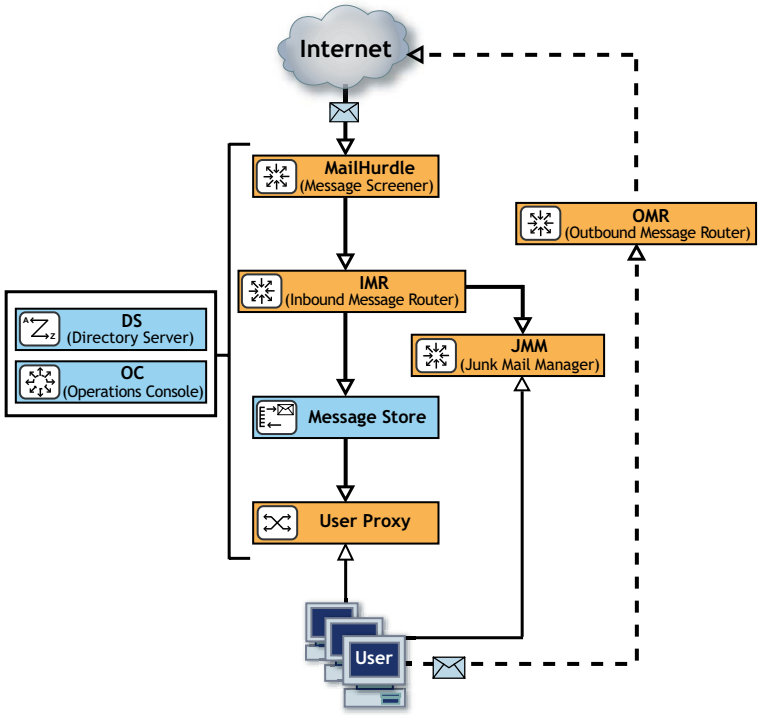

Figure 2 Mirapoint Security and Messaging Functions

Inbound messages are first screened by MailHurdle. MailHurdle performs pre-acceptance screening of messages by only accepting messages from recognized sources. Those that pass MailHurdle's pre-acceptance screening are then passed on to the Inbound Message Router (IMR). The IMR filters the messages and scans them for viruses and spam. The IMR then accesses the Directory Server to determine where to deliver each message. The Directory Server is an LDAP directory that performs user authentication and management for the messaging infrastructure. Finally, the message is sent to the recipient's mail folder on the appropriate Message Server. The Message Server stores and serves messages and provides access to additional collaboration tools such shared calendars and address books.

When Junk Mail Manager (JMM) is used, messages that are determined to be spam can be diverted to the JMM quarantine before reaching the recipient's mail folder. The JMM quarantine provides a separate storage area for suspect messages to avoid clogging user folders with spam.

When a user logs in, the Directory Server is accessed to authenticate the user. If the deployment includes multiple Message Servers, the connection is redirected to the appropriate Message Server by the User Proxy. The User Proxy makes the existence of multiple Message Servers transparent to the user—all users sign into the server acting as the User Proxy regardless of which server their mail folders actually reside on.

Outgoing messages are routed to the appropriate destinations by the Outbound Message Router (OMR).

While these functions can be performed on a single appliance, you can distribute them to:

- Increase capacity and performance
- Minimize the impact of incoming attacks
- Minimize the impact of outbound attacks
- Manage increases in spam and virus loads

This section takes a closer look at each of these functions and the situations in which it makes sense to split them off into separate tiers in your messaging infrastructure.

MailHurdle Function

MailHurdle screens inbound messages at the edge of your network to determine whether or not they should be accepted. Only connections from recognized senders are accepted, eliminating the majority of spam traffic before it ever enters your network.

MailHurdle can reside on the same tier as the IMR, but is sometimes split off to optimize inbound message handling. Splitting the pre-acceptance screening function off into a separate tier can reduce the load on the IMR by as much as 75%. Where you might need five RazorGate 500 appliances to handle the message load when the screening, scanning, and routing functions are combined on the same tier, you could handle the same load with 5 RazorGate 100 appliances in the screening tier and just two RazorGate 500s in the inbound routing tier, saving both money and rack space.

Inbound Message Router Function

The Inbound Message Router (IMR) filters incoming messages, performs spam and virus scanning, and then determines where the messages should go.

The IMR function can be combined with the MailHurdle message screening function. Separating the IMR from MailHurdle (a so-called split-IMR configuration) is advantageous when there's a large spam or virus load. Pre-acceptance screening can be performed by a separate tier of RazorGate 100 appliances, saving money and rackspace by reducing the load on the RazorGate 350/500 appliances in the IMR tier.

Junk Mail Manager Function

The Inbound Message Router can direct messages flagged as spam to the Junk Mail Manager (JMM) instead of the user's Inbox. Using JMM prevents spam from clogging up your message servers while still enabling individual users to manage their quarantined junk mail.

JMM periodically sends users a personal Junk Mail Summary. Users can choose to release any of the quarantined messages they want to receive. When a user accepts a quarantined message, it is delivered to their mail folder and the message sender is added to the allowed senders list. Users do not have to take any action on

quarantined messages. If messages are not accepted within a set period of time, they automatically expire and will be deleted to free up space in the quarantine.

JMM must be deployed on a RazorGate appliance, it cannot reside on a Message Server. JMM can reside on the same tier as the IMR, but if there is a large volume of quarantined messages, it should be split off into a separate tier. JMM is not available when you're using an all-in-one configuration.

The JMM is placed inside the firewall where it is accessible to the RazorGate appliances for routing, and to users for optional login. The LDAP directory is used to route spam to the user's JMM quarantine folder and send valid messages on to the Message Server for delivery.

Outbound Message Router Function

The Outbound Message Router (OMR) authenticates the sender using SMTP auth to ensure the user is local, makes sure the outgoing message contains the correct MAIL FROM: information, and can optionally screen the outgoing message for spam and viruses.

The OMR is typically split off into a separate tier to prevent inbound spam attacks from affecting outgoing traffic or when there is a high risk of users being a source of spam. When the OMR and IMR functions are separated, users can still access and send messages during inbound attacks and receive and access messages during outbound spam attacks.

Message Server Function

The Message Server is the foundation of the messaging infrastructure, serving, securing, and managing messages. A Mirapoint deployment can be built around a Mirapoint Message Server appliance or integrate existing message servers such as Microsoft Exchange or Lotus Notes.

In all but the simplest configurations, the routing and proxying functions are typically split off from the Message Server tier. In small deployments the Directory Server and Operations Console functions reside on the same tier as the Message Server. For larger user communities and message loads, the Directory Server and Operations console are also split off from the Message Server.

Directory Server Function

The Directory Server is an LDAP server that stores and manages user profiles, access privileges, and message routing information. The Directory Server is the backbone of the messaging infrastructure, providing unified user and system management for all messaging functions.

The Directory Server can be combined with the Message Server tier, or split off into a separate tier. If you have a large number of users, you generally want to split off the Directory Server function so that the LDAP query volume does not impact email performance on the Message Server.

When a deployment integrates an existing Exchange Server, Active Directory functions as the Directory Server for the messaging network.

User Proxy Function

The User Proxy determines where a user's message store is located and redirects the connection during login. Both IMAP and POP connections can be proxied, in addition to HTTP for WebMail and WebCal.

The User Proxy function is often grouped with the OMR function in a single tier. However, in environments where there is a high risk of users being a source of spam, user proxying can be split off from the OMR so that user access to the message network is not affected by outbound spam attacks.

Operations Console Function

The Operations Console (OC) enables you to centrally manage a group of Mirapoint appliances. The load generated by the OC is minimal and it typically resides on the same tier as the Directory Server.

Keep in mind that the OC does maintain persistent data and needs to be on an appliance with a persistent data store that is routinely backed up.

Mirapoint Messaging Reporter Function

The Mirapoint Messaging Reporter (MMR) is a Microsoft Windows application that lets administrators effectively manage email security information and events.

MMR automatically collects device log files, normalizes data across disparate devices, and aggregates all this data into a database.

MMR then correlates the data for monitoring, alerting, reporting, and forensic tasks.

2 Mirapoint Deployment Scenarios

How you deploy a Mirapoint messaging solution depends primarily on the number of users and volume of messages you need to support. Mirapoint's multi-tier architecture enables the various components in the messaging network to be distributed as needed to accommodate an organization's message traffic. As the demands on the messaging network grow, additional appliances can easily be added and the messaging network adjusted to optimize capacity and performance.

In the simplest deployment scenario, a single Mirapoint appliance can provide an all-in-one messaging and security solution. However, by distributing the Mirapoint's security and messaging functions across a collection of RazorGate and Message Server appliances, you can scale your messaging network to support an extremely large volume of messages and users.

This chapter describes the different options you have for deploying Mirapoint's security and messaging functions within your network.

Deployment Options

There are three main types of Mirapoint deployments:

- All-in-One: A Mirapoint Message Server deployed as an all-in-one messaging and security solution. Suitable when the number of users is under 1000 and Junk Mail Manager functions are **not** required.
- RazorGate Security: Mirapoint RazorGate appliances deployed to secure a messaging infrastructure that includes a Mirapoint Message Server or other mail store such as Microsoft Exchange. Suitable if you need to integrate with an existing Exchange Server.
- Mirapoint Multi-Tier: Mirapoint RazorGate and Message Servers deployed to provide a total messaging solution; may also be configured with Exchange as the mail store. Suitable if the number of users is 1000 plus, or you want to use JMM to quarantine spam.

The following sections describe each of these scenarios in detail.

All-In-One Scenario

In an all-in-one deployment, a Mirapoint Message Server appliance provides everything an organization needs to deliver email services to up to 1000 users. This

is the simplest Mirapoint solution to deploy and maintain and is ideal for small organizations.

Selecting the All-in-One Deployment

A Mirapoint all-in-one deployment is appropriate when:

- The total number of users will not exceed 1000.
- Sending spam to a dedicated quarantine server is **not** required.

All-in-one deployments do not include the Mirapoint Junk Mail Manager (JMM) functionality. If you want to divert messages flagged as spam to a dedicated server rather than flagging and delivering them to your users, you will need to deploy a multi-tier solution that includes JMM. For more information see Mirapoint Multi-Tier, Multi-Appliance Scenario on page 26.

Understanding All-In-One Deployments

In an all-in-one deployment, all of the Mirapoint security and messaging functions can reside on a single Message Server appliance. The Message Server functions as a connection MailHurdle, antivirus scanner, antispam scanner, message store, calendar service, mail client server, directory server, and outbound message router.

Figure 3 shows how an all-in-one solution fits into your network.

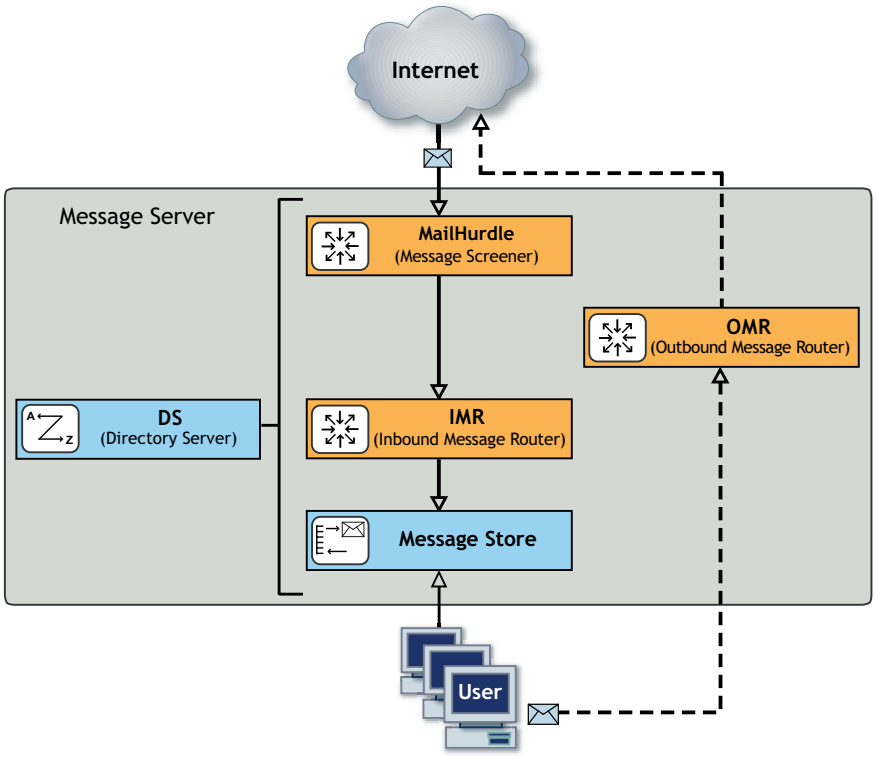

Figure 3 Mirapoint's All-in-One Deployment Scenario

Once deployed, the Message Server handles and secures all of your incoming and outgoing email. Users can send and receive email via IMAP, POP, or WebMail. They

can access calendaring functions via WebCal or Outlook/SynQ. Directory server LDAP unctions can be handled internally (Internal Directory) or by Active Directory on a Microsoft Exchange server.

Expanding an All-in-One Deployment

Should your user population grow and you need to increase capacity and performance, you can always expand your all-in-one deployment by adding additional appliances in a multi-tier configuration.

For example, you might initially deploy a RazorGate tier at the edge of your network to offload screening and routing functions from your Message Server. As the demands on your messaging network increase, you can further distribute security, routing, and messaging functions to meet your capacity and performance requirements.

For more information about distributing functions across multiple tiers, see Mirapoint Multi-Tier, Multi-Appliance Scenario on page 26.

RazorGates Security Scenario

In a RazorGate Security deployment, Mirapoint's RazorGate appliances are used to secure incoming email; at least two should be used to provide failover protection. Message handling is performed by a separate messaging server, such as Microsoft Exchange, or a Mirapoint Message Server (MMS) or Directory Server. The RazorGates Security deployment option enables you to integrate Mirapoint's unparalleled multi-layered protection from spam, virus, and hacker attacks into your existing messaging network.

Selecting the RazorGates Security Deployment

A Mirapoint RazorGate Security deployment is appropriate when the messaging network includes an MMS or Exchange server that performs the message handling functions.

Multiple RazorGate appliances can be deployed as needed to accommodate the expected number of users and message traffic; at least two are required for this deployment. If you want to divert spam to a dedicated quarantine server to reduce the load on your mail server(s), one of the RazorGates can be configured as a Mirapoint Junk Mail Manager (JMM).

Understanding RazorGates Security Deployment

In a RazorGate Security deployment, Mirapoint's security functions reside on two or more RazorGate appliances at the edge of your messaging network. The RazorGate appliances function as inbound and outbound message routers, perform message screening, apply filters, and scan for spam and viruses.

Figure 4 shows how a basic RazorGates solution fits into your network.

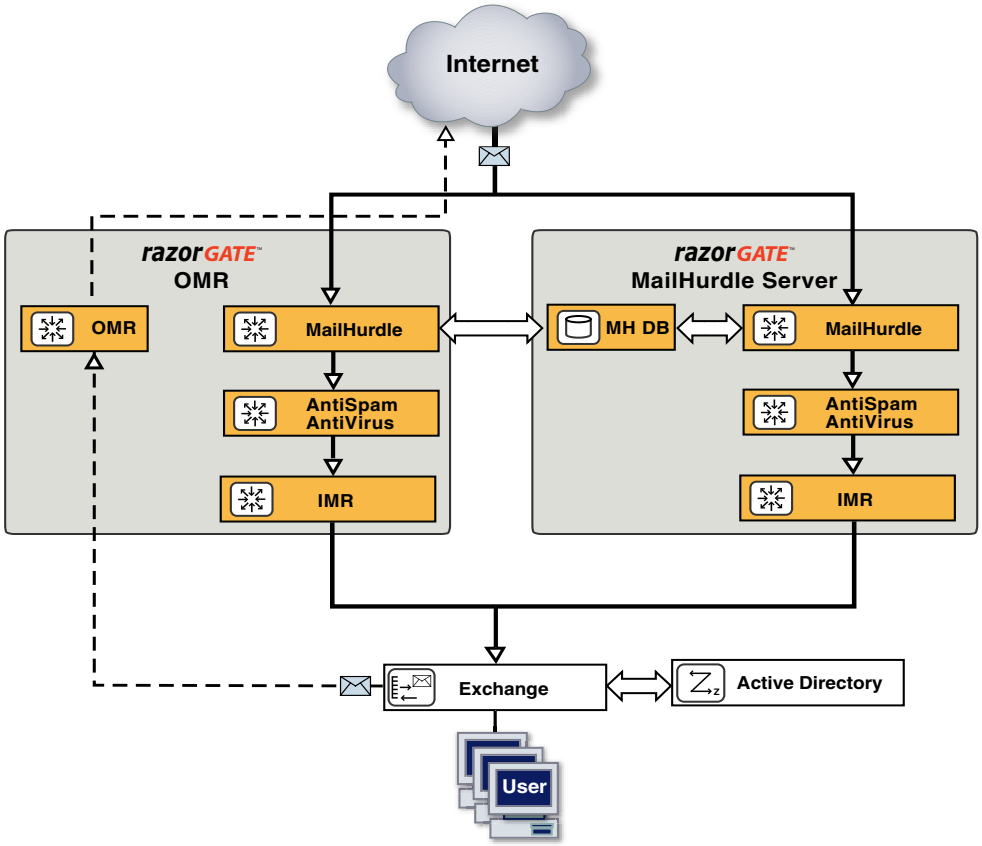

Figure 4 Mirapoint RazorGates Appliances Securing Exchange

RazorGate appliances can perform inbound and outbound message routing for multiple mail servers. Internal Directory on an MMS or Mirapoint Directory Server, or Active Directory on an Exchange server, is used to look up the assigned mail host for each user.

Using JMM in a RazorGates Security Deployment

In a standard RazorGates Security deployment, all messages passed through by the MailHurdle are scanned for spam. Suspect messages are then flagged as spam by modifying the message subject, or (for IMAP users) sent to an IMAP JunkMail folder.

When Junk Mail Manager (JMM) is added to the messaging network, at least 90% of spam messages are diverted to the JMM quarantine, substantially reducing the message load on your mail servers. Individual users can access the quarantine to view or release messages and specify preferences for how their spam is handled. Figure 5 shows how JMM fits into a RazorGates deployment.

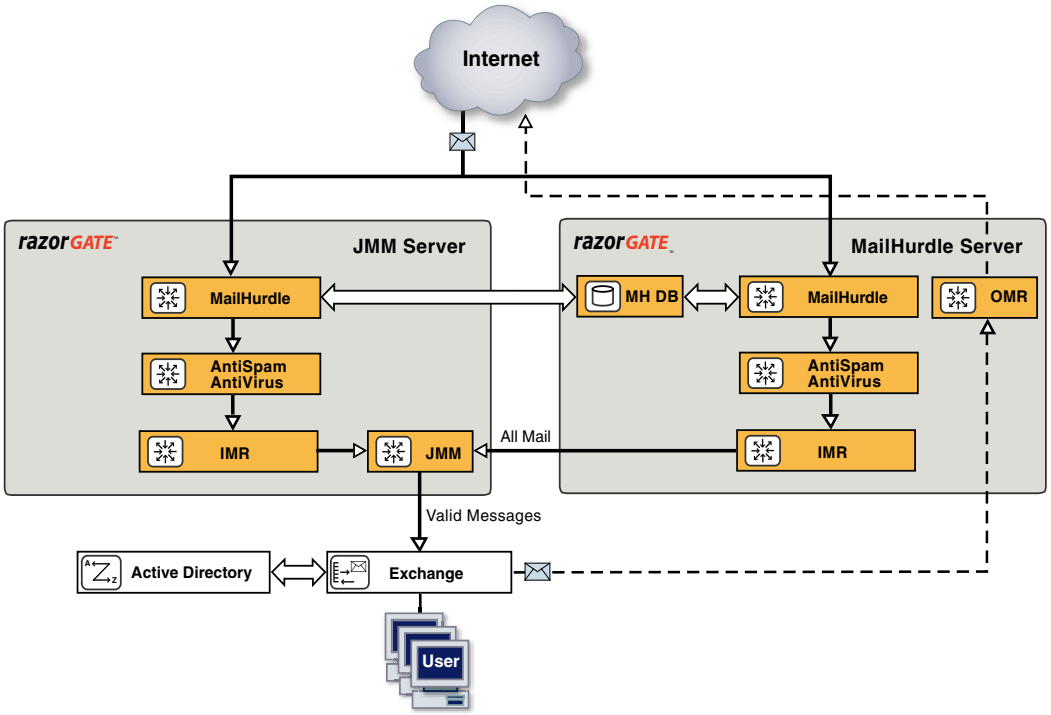

Figure 5 RazorGate Scenario with JMM and Active Directory with Exchange

The RazorGates use Active Directory or Mirapoint Internal Directory to route spam to the user's JMM quarantine folder and send valid messages on to the mail server for delivery.

Load Balancing

To share the load between a pair of RazorGate appliances at the edge of your network, you can assign equal MX records to both appliances. By assigning the same priority in MX records for both servers, incoming messages are randomly assigned to one of the two servers. If either becomes unavailable, DNS routes to the still-active appliance. For example:

```
example.com   MX preference = 5, mail exchanger = imr1.example.com
example.com   MX preference = 5, mail exchanger = imr2.example.com
```

Alternatively, you could deploy an OSI Layer-4 load balancer in front of the RazorGate appliances for intelligent, non-random load balancing.

Expanding a RazorGates Security Deployment

A RazorGates Security deployment can be split into multiple tiers to increase performance and capacity as the number of users grows and message volume increases. The MailHurdle function and the inbound and outbound message routers can all be separated.

For example, if the volume of inbound email is affecting users' ability to compose and send, it's time to split off the outbound message router into a separate tier.

If scanning load gets too high, or headroom during spam storms gets tight, you can deploy two RG100 MailHurdle appliances in front of the RazorGate appliances. By eliminating the majority of spam traffic before it ever enters your network, they significantly reduce load on the RazorGate appliances.

For more information about splitting the security and routing functions into multiple tiers, see Distributing Security and Routing Functions on page 29.

Mirapoint Multi-Tier, Multi-Appliance Scenario

In a Mirapoint Multi-Tier deployment, a combination of RazorGate and Message Server appliances form a complete messaging network. Mirapoint's security functions reside on one or more RazorGate appliances at the edge of your network, and messages are handled and delivered by Mirapoint's Message Server (MMS). A Mirapoint Multi-Tier deployment provides the flexibility and scalability to handle virtually any size user community and message load.

The biggest factors in determining how to distribute Mirapoint's security and messaging functions within your messaging infrastructure are the number of users and message volume that you need to support. If you do not have this information available, contact your Mirapoint sales representative for assistance in evaluating your messaging requirements and projected loads.

Selecting a Mirapoint Multi-Tier Deployment

A Mirapoint Multi-Tier deployment is appropriate when you:

- Need a complete security and messaging solution.
- Have more than 1000 users.
- Have fewer than 1000 users, but you want to use Mirapoint's Junk Mail Manager to divert spam to a separate quarantine.

Understanding Multi-Tier Deployments

Multi-tier deployments offer a scalable messaging solution that can seamlessly integrate as many RazorGate and Message Server appliances as needed to deliver the capacity and performance your organization requires.

In a multi-tier deployment, security and routing functions are performed by one or more RazorGate appliances, while Message Server appliances take care of the message handling and delivery. Figure Figure 6 shows how the specific functions

described in Deployment Options on page 21 are distributed between RazorGate and Message Server appliances:

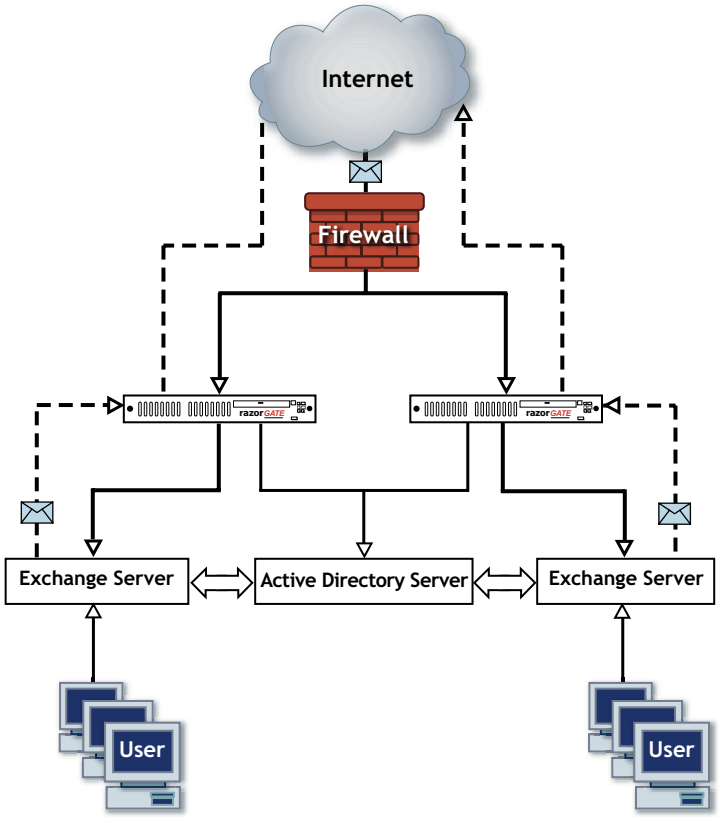

Figure 6 RazorGate and Message Server Functions Using Exchange

The simplest deployments have just two tiers:

- The appliances in the RazorGate tier perform all security, routing, and proxy functions.
- The appliances in the Message Server tier perform the directory service, message store, and operations console functions.

See Figure 7 on page 28 for an illustration.

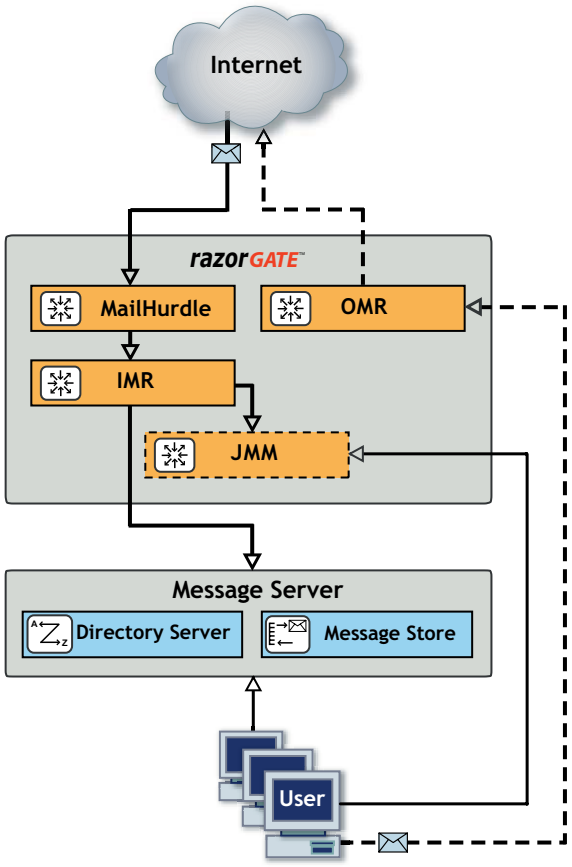

Figure 7 Two-Tier Deployment

The initial deployment for a medium-sized organization is usually based on this basic two-tier architecture. For example, Figure 8 shows a two-tier deployment with two RazorGate appliances performing the tier 1 security and routing functions

and two Message Servers performing the message store and directory service functions.

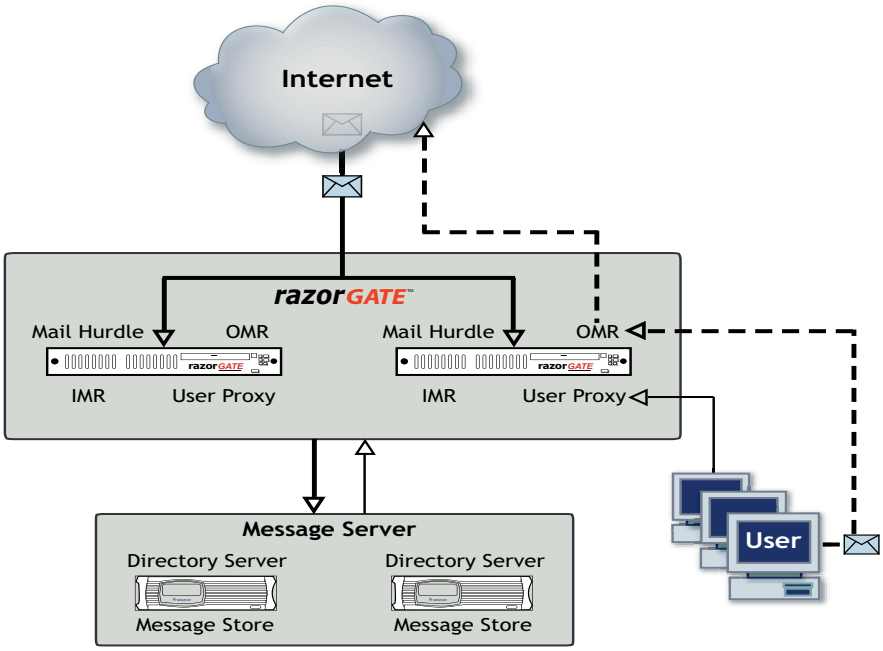

Figure 8 Initial Deployment for a Medium-Sized Organization

Distributing Security and Routing Functions

The RazorGate security, routing, and proxy services can distributed across additional tiers to increase capacity and performance.

Splitting Off Outward-Facing Security Functions

The first step is usually to split the outward-facing security and routing functions off from the inward-facing routing and proxy functions, as shown in Figure 9:

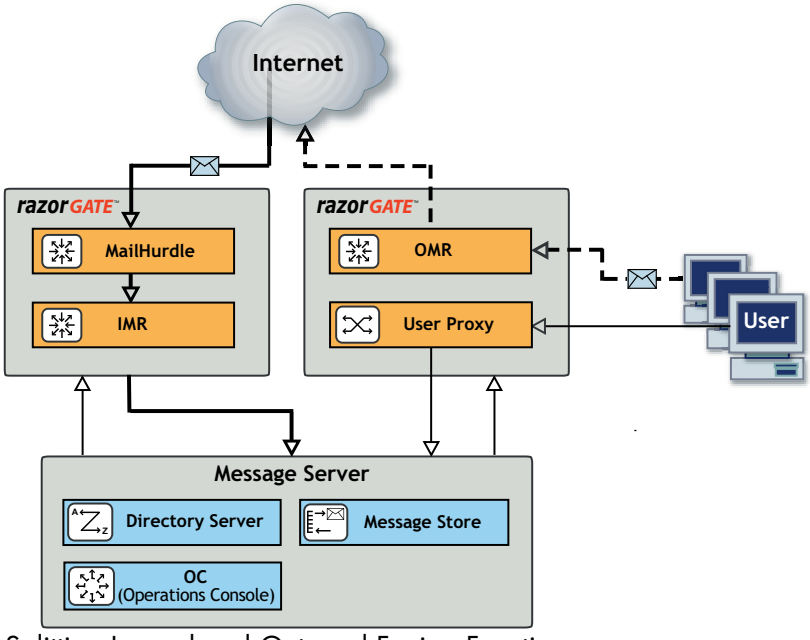

Figure 9 Splitting Inward and Outward Facing Functions

Separating the OMR and Proxy functions from the IMR and MailHurdle functions prevents Internet attacks or a large incoming message load from affecting your users' ability to access and send messages. Moving to this type of deployment scenario is advantageous when the volume of inbound spam is affecting the capability of the users to access and send mail.

Splitting Off MailHurdle Functions

If you have a large amount of incoming spam or virus-infected messages, you should separate the MailHurdle pre-acceptance scanning functions from the IMR that performs the filtering, anti-spam, anti-virus, and routing functions. This is illustrated in Figure 10.

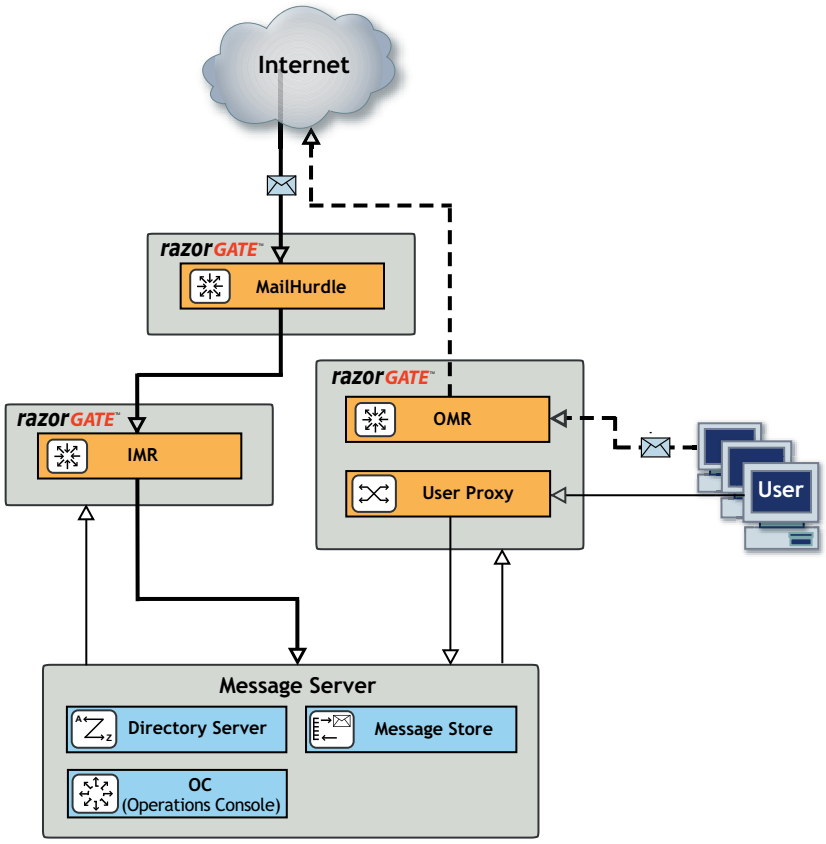

Figure 10 Splitting the MailHurdle and IMR Functions

Splitting the MailHurdle and IMR functions is useful in large service provider deployments. This deployment scenario enables you to use a tier of cost-effective RG-MH appliances at the edge of your network as gatekeepers and significantly reduce the load on the RG 350/500 appliances that perform the in-depth processing of inbound messages. (A load reduction of 75% on the IMR is not uncommon.)

Distributing Message Store and Directory Server Functions

As the number of users and the overall message volume increase, the number of LDAP queries increase. If the resulting load on the Message Server tier affects the user experience, the Directory Server should be split off into a separate tier.

Generally, if you have four or more appliances performing LDAP lookups, you should have a dedicated Directory Server tier, as shown in figure Figure 11.

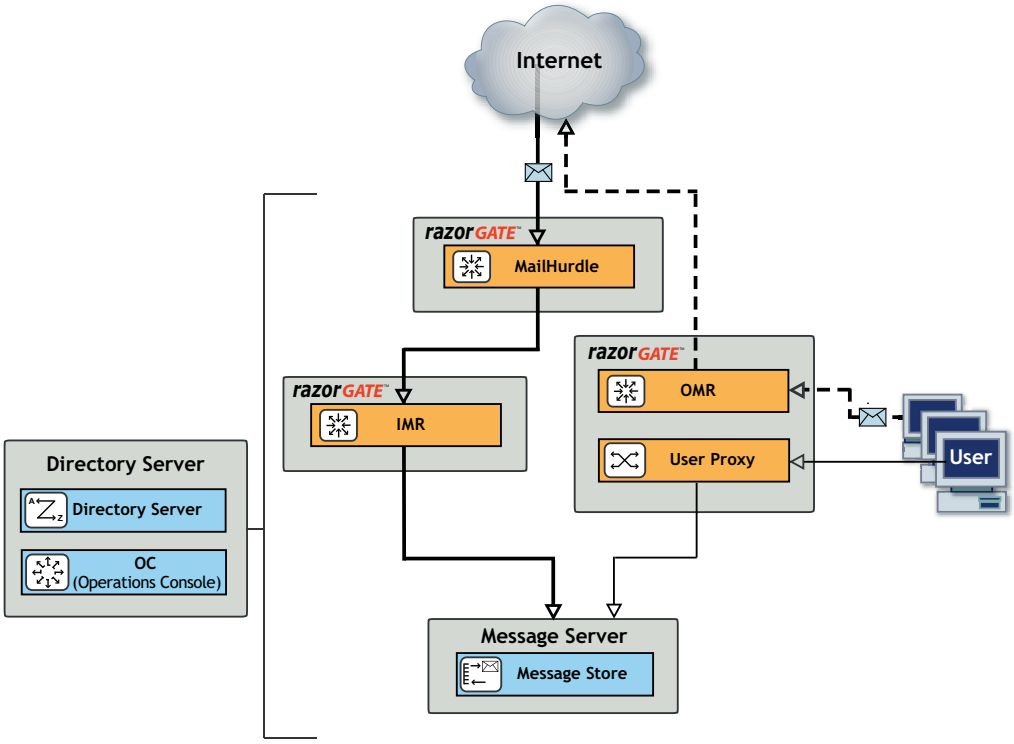

Figure 11 Splitting Directory Server and OC from the Message Store

When the Directory Server function is split off from the Message Server, the Operations Console generally resides in the Directory Server tier.

Splitting Off User Proxying

You can also split user proxying off from the outbound message routing functions, as shown in figure Figure 12:

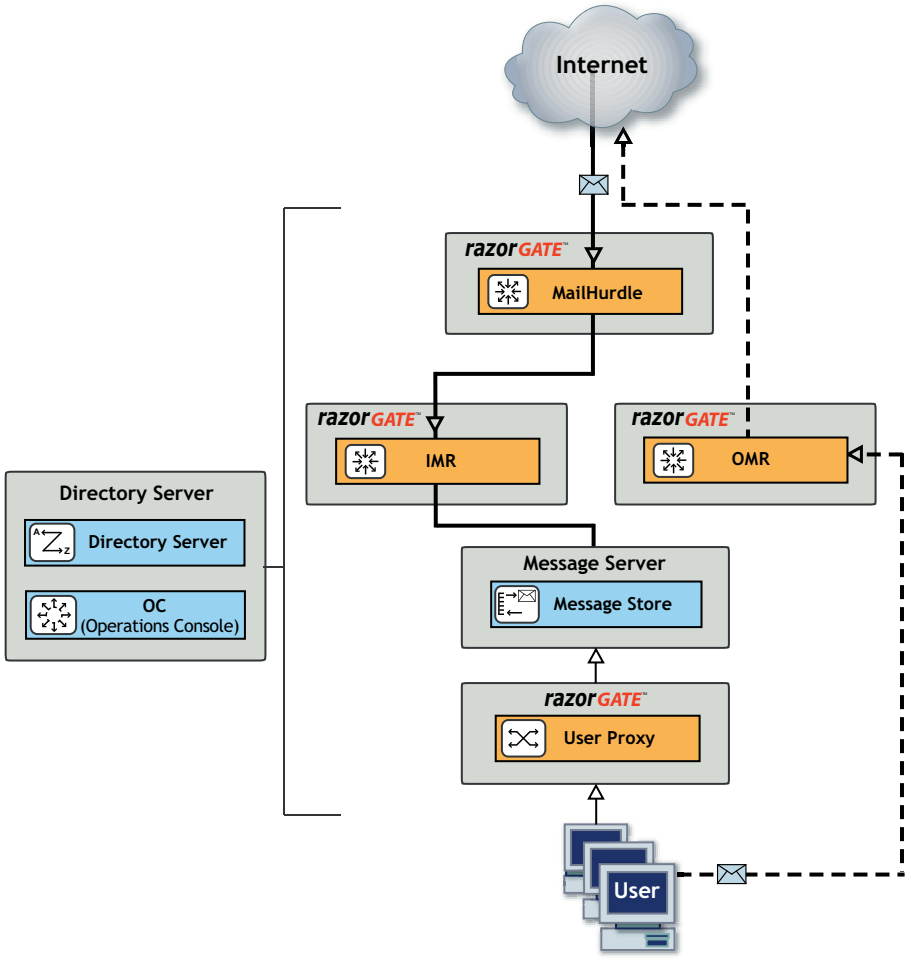

Figure 12 Splitting the User Proxy and OMR Functions

Separating the user proxy and OMR functions ensures that your users will still be able to access the message network in the event of an outbound spam attack. This is particularly useful in educational or ISP settings where there is a high risk of your users being a source of spam. While load conditions might affect your users' ability to send messages, they will still be able to access incoming messages.

Configuration Considerations: In a typical implementation, the user proxy and OMR functions reside behind a single layer 4 load balancer. The load balancer directs Port 25 SMTP traffic to the outbound message router cluster, and ports 80, 110, 143, 443, 993, and 995 are directed to the proxy cluster.

Using JMM in a Multi-Tier Deployment

In a standard multi-tier deployment, all messages passed through by the MailHurdle are scanned for spam. Suspect messages are then flagged as spam by modifying the message subject, or (for IMAP users) sent to an IMAP JunkMail folder.

Junk Mail Manager (JMM) can be added to the messaging network to divert spam messages to the JMM quarantine and substantially reduce the load on your Message Servers. Individual users can access the quarantine to view or release messages and specify preferences for how their spam is handled. Figure 13 shows how JMM fits into a multi-tier deployment.

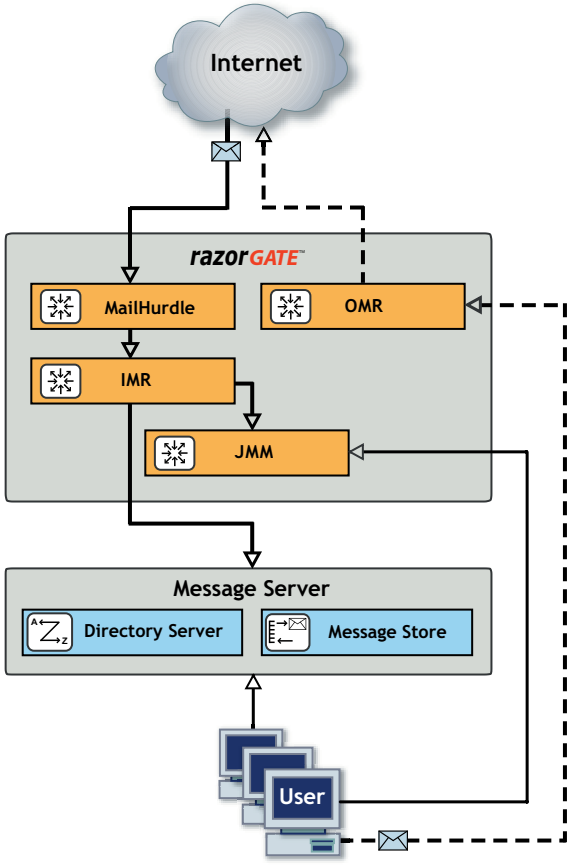

Figure 13 JMM Combined with the IMR Tier

JMM can reside on the same tier as the IMR, but if there is a large volume of quarantined messages, it should be split off into a separate tier, as shown in Figure 14.

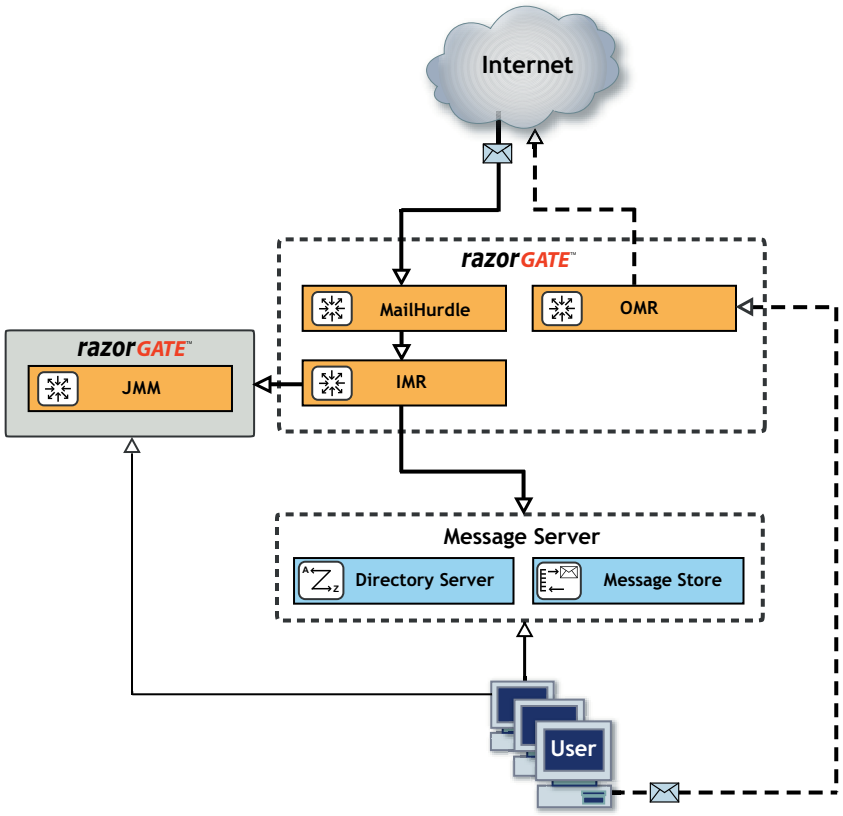

Figure 14 Splitting JMM and the IMR

3 Planning for Deployment

Once you know what appliances will form your new messaging infrastructure and how you will distribute functions among those appliances, you can plan how to integrate them into your network, test your deployment choices, and schedule a "go-live" date.

Keep in mind that your installation site must have:

- An air-conditioned data center
- Grounded electrical power source with local voltage
- Ethernet connectivity
- Space in your four-rail rack to accommodate the appliances

See the Mirapoint hardware documentation for detailed installation requirements and procedures.

Integrating Mirapoint Systems into Your Network

To support a Mirapoint deployment, your network infrastructure needs to have the following services available:

- DNS (Domain Name System) Services: Naming services that translate IP address to host and domain names.
- NTP (Network Time Protocol) Services: Assures accurate local timekeeping with reference to clocks located on the Internet. (External NTP servers such as **0.pool.ntp.org** can be used for synchronization.)
- Directory Services (recommended): A structured repository of information on people and resources within an organization, facilitating management and communication; usually managed with LDAP (Lightweight Directory Access Protocol)

- Mirapoint also recommends that your network infrastructure includes a firewall to filter incoming network traffic.

Like all network servers, Mirapoint appliances need to be assigned an IP address, hostname, netmask, router, domain name, and DNS servers. Initial values for these network parameters are set using the console interface during the hardware installation process.

About Domain Name System (DNS)—Naming Services

Your organization may control its own DNS services, or an ISP might do this for you. Either way, add these DNS records for each appliance:

- "A" record: Maps host name to IP address, required
- "PTR" record: Maps IP address to host name, required
- "MX" record: Mail exchange record, required for every domain
- "CNAME" record: Establishes a host alias (alternate name), optional

For more information about DNS, see the Wikipedia Domain Name System article.

About Network Time Protocol (NTP)—Clock Time Services

Because every step of message delivery inserts a timestamp, and because messages delivered to a folder usually appear in chronological order, it is important to have the correct time set on all messaging appliances. The recommended way to coordinate date and time among appliances is with NTP (network time protocol). You can set the NTP server and timezone with Setup Wizard.

For more information about NTP, see the Wikipedia Network Time Protocol article.

About Directory Services

An LDAP directory server is used to provide user authentication and management services for Mirapoint messaging. You can use a Mirapoint Directory Server or any LDAP v.3 compliant server, such as Microsoft Active Directory or Novell eDirectory.

If you use a third-party directory server, the user and domain schemas need to be extended to support Mirapoint features. The schema extensions are available for download from Mirapoint Support and conform to RFC 2252. If your directory server does not understand the attribute syntax described in RFC 2252, the schema will need to be converted. For more information about the Mirapoint schema extensions, visit Mirapoint Support.

About Firewalls

For a Mirapoint deployment, your network will generally include a firewall that filters incoming network traffic to prevent unwanted packets and protocols from intruding onto your internal network.

In configurations that include a firewall, you should generally only allow mail traffic to reach your IMR/MailHurdle devices and block all other traffic.

Many networks use two firewalls to create a DMZ (de-militarized zone) between the Internet and the internal network. Hosts that need to be accessible from the outside world are placed within the DMZ. Connections to hosts within the DMZ

are permitted from either the internal or external networks, but hosts within the DMZ can only initiate connections to the external network.

RazorGate security appliances reside inside the Firewall at the very edge of your network, as shown in Figure 15. RazorGate MailHurdle typically lies within the DMZ if you have one. Message Server and Directory Server appliances should reside on your internal network, they do not need to be within the DMZ.

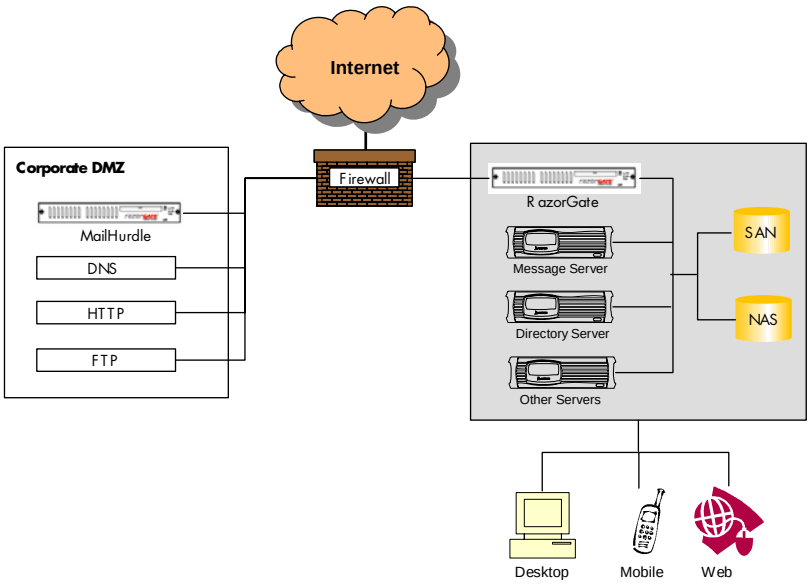

Figure 15 Mirapoint Secure Messaging Infrastructure

Configuring Your Firewall

You must configure your firewall to allow messaging traffic.

Table 3 shows which ports you might need to open for inbound connections to support basic Mirapoint services. Table 4 shows ports to open for outbound connections.

Mirapoint recommends configuring your firewall to close off all connections in the range 1034-65535 for UDP. Some TCP ports in this range (as specified in Table 3 and Table 4) should be left open.

Table 3 Open Ports for Inbound Connections

Port Number	Type	Service Name	Service Description	Use
22	TCP	SSH	Secure Shell	Open to enable remote administration, if SSH is licensed.
25	TCP	SMTP	Simple Mail Transfer Protocol	Open to allow SMTP traffic to the devices operating as MailHurdle or first point of entry.
80	TCP	HTTP	HTTP	Open to support Web browser access for remote users.
110	TCP	POP	Post Office Protocol 3	Open to support external POP3 clients for remote users.
143	TCP	lMAP	Internet Message Access Protocol	Open to support external IMAP4 clients for remote users.
443	TCP	HTTPS	Secure HTTP	Open to support secure HTTP connections for remote users, if licensed.
993	TCP	IMAP SSL	Secure IMAP4	Open to support external secure IMAP clients for remote users, if licensed.
995	TCP	POP SSL	Secure POP3	Open to support external secure POP clients for remote users, if licensed.

To support client connections from remote users, Mirapoint recommends blocking the standard HTTP, IMAP, and POP protocols and only allowing inbound connections via the corresponding secure protocols (Open ports 443,993 and 995, but not 110, 143, and 80).

Table 4 Open Ports for Outbound Connections

Port Number	Type	Service Name	Service Description	Use
21	TCP	FTP	File Transfer Protocol	Open to enable the retrieval of software updates.
25	TCP	SMTP	Simple Mail Transfer Protocol	Open to allow SMTP traffic.
80	TCP	HTTP	HTTP	Open to enable the retrieval of anti-virus and anti-spam updates.

Table 4 Open Ports for Outbound Connections (Continued)

Port Number	Type	Service Name	Service Description	Use
53	TCP	DNS	Domain Name System	Open to enable DNS queries.
123	UDP	NTP	Network Time Protocol	Open to support date/time synchronization.

Mirapoint recommends only allowing the OMR to transmit SMTP to the Internet. All other servers should go through the OMR. This enables you to enforce outbound email policies.

For more information about the ports used by Mirapoint appliances, see Knowledgebase Article #66 on the Mirapoint Support Website.

Table 5 Mirapoint Supported Browsers

For Windows systems	❖ Firefox 1.0 and above (Mozilla 1.7 and above) ❖ Netscape Browser 7.1 and above ❖ Microsoft Internet Explorer 6.0 and above
For Macintosh systems	❖ Safari 1.2 and above

4 Security Features Overview

The goal of messaging security is to deliver the messages that users want to receive, and not deliver messages they don't want to receive, while screening out harmful viruses. This is not as simple as it sounds because spam and viruses can be disguised many different ways.

This chapter helps you understand messaging and security terminology and what tasks are required to implement Full-Spectrum™ technology on RazorGate and Mirapoint appliances.

RazorGate Configurations

If your organization already has message routers that deliver email wherever user's mail folders reside, you can deploy RazorGate appliances as message screeners to perform connection MailHurdle, antivirus scanning, antispam scanning, and content filtering. If this is the case, configure RazorGate appliances SMTP service to use "local message router" (LMR). Exchange Bridgehead is one example of an LMR.

If your organization has no LMR, or wants to replace it, you can have RazorGate appliances route messages, optionally using LDAP, after doing the security checks described above. If this is the case, configure RazorGate appliances as routers, using either "local routing table" or one of the "LDAP routing" options.

What configuration in which deployment?
Every security feature described in this chapter can be configured on all RazorGate appliances, except where noted. If you split off inbound or outbound message router onto a separate box, then security features in those respective sections should be configured on that router.

Layers of Messaging Security

As messages arrive from the Internet into your network, Mirapoint software offers the following security layers:

- Network Security—Firewall style features.
  This includes denial-of-service protection, mail server verification via reverse DNS, blocking problematic networks or domains, and avoidance of open relays.
- Inbound Message Handling—How SMTP responds.
  During email transmission by SMTP, many security decisions are made, such as:

identifying DNS address, whether to encrypt the connection, mail client authentication, sender check, recipient check, and mailer integrity verification. At this layer, verifying mailer integrity with MailHurdle is a currently a highly effective spam and virus reduction method.

- Message Content Control—Decides what not to deliver.
  This layer includes high-priority content filters, antivirus scanning to eliminate harmful viruses, antispam scanning to dispose of unwanted messages, system content filters, allowed senders lists, blocked senders lists, and user content filters. All content filters have similar syntax and implementation but can be called at different stages.
- Message Routing—Delivers to appropriate mail server.
  After verification of messages, they are routed and delivered to users, usually on a different computer or possibly a different network. RazorGate appliances can be placed inside or outside the firewall depending on network configuration. Spam can be delivered to Junk Mail folders or marked as spam in the subject header line. Mirapoint software provides different ways to monitor email security, including graphs and logs.
- Outbound Message Control—Outgoing message content.
  This layer is similar to message content control, but on the way out. Names and addresses can be normalized. Forgeries can be controlled by sender validation.

Figure 16 on page 43 shows the progression of a message through the various security layers. Figures starting on page 44 show flowcharts for each security layer.

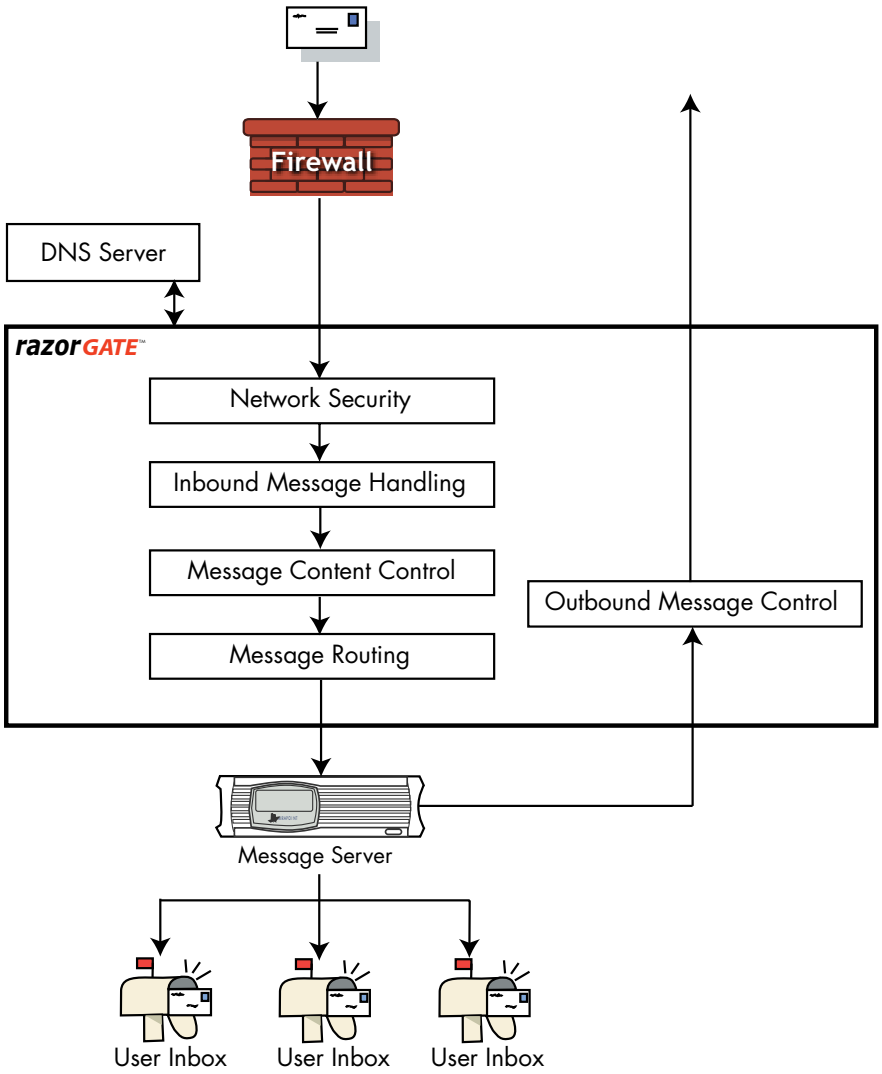

Figure 16 Message Security Processing

Security Features

Security features are presented below, arranged from the outside in. This is just organizational; you can administer features in any order.

Network Security

RazorGate offers firewall-style features to enforce network security. See Figure 17 for a flowchart of this layer.

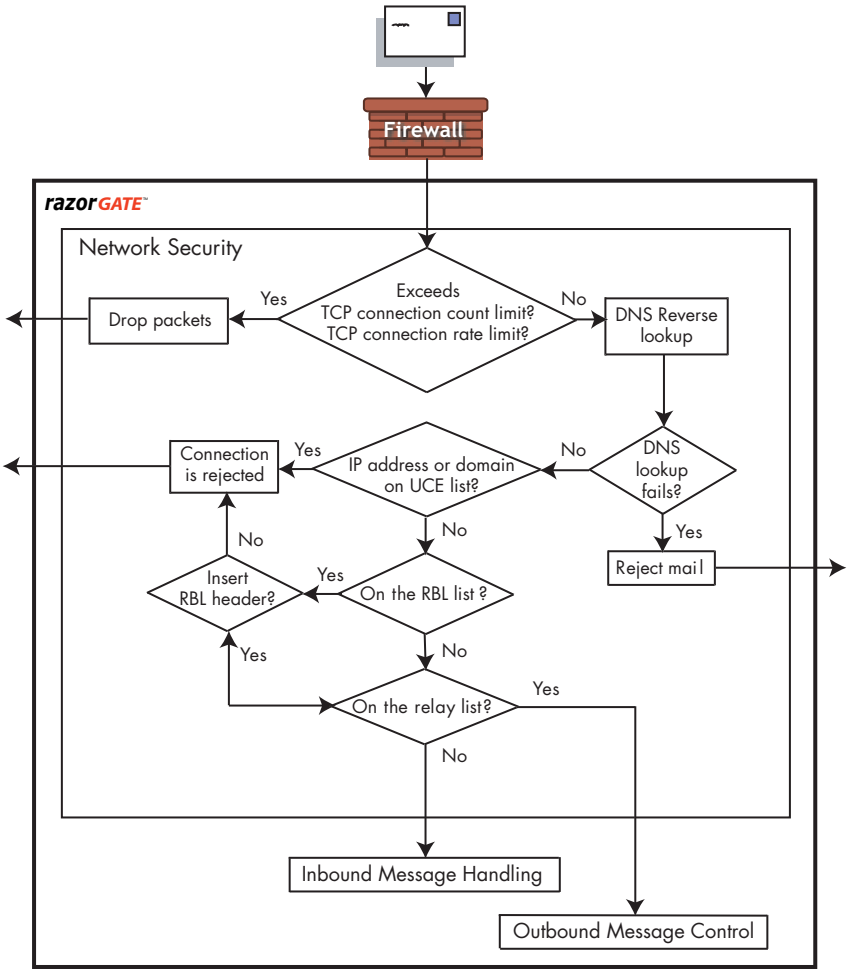

Figure 17 Network Security Layer

Denial of Service Prevention

In a denial-of-service attack, systems are overwhelmed by requests from a small set of sources, slowing down response time and reducing bandwidth for bonafide users.

You can help prevent denial-of-service attacks by limiting the number of TCP connections and the connection rate. This is done by enabling Denial of Service Prevention on the point of entry to your messaging network—typically the servers that are running MailHurdle.

Once Denial of Service Prevention is enabled, the TCP connection count limit is 50 and the connection rate limit is 400 per ten seconds. You can adjust these limits and exclude selected hosts from the limits by making them trusted hosts.

If you limit the number of TCP connections and the connection rate, you should determine which SMTP servers send the most mail to your site and make them trusted hosts. Otherwise, setting these limits will delay messages from your high-traffic sources.

Reverse DNS Verification

When a mail server connects to RazorGate's SMTP port, messaging software notes the numeric IP address of the originating mail server, and looks up that number to find its corresponding alphabetic address. If this so-called reverse DNS lookup fails, the SMTP service delays response to further requests from that IP address. After reverse DNS verification, Mirapoint SMTP offers this greeting:

```
250 m1.example.com Hello msg.net [192.168.9.84], pleased to meet you
```

This is always done on Mirapoint servers, and cannot be disabled.

Network and Domain Rejection

Once SMTP service has identified the connecting IP address and its fully qualified DNS host name, you can have it reject specific domain names or networks. To block an entire network, give a partial IP address. To block a DNS domain, give the domain name. This is called the "Reject" list, or UCE list (unsolicited commercial email, an acronym for spam).

Unless you know immediately which hosts and networks to block, it is preferable to let DNSBL (see below) and MailHurdle (if licensed, see page 49) handle this issue. However, when the Mirapoint logs suggest that a large amount of spam is incoming from a single source, use the UCE list to block that server.

Open Relay Prevention

Relaying is the transfer of messages from one remote server to another. This is how RazorGate appliances deliver mail from the Internet to your site, and from your site's systems to the Internet. That is valid relaying. However you do not want to relay mail from unknown remote systems. This is called open relaying. It leaves servers open to highjacking.

Mirapoint software does not permit open relaying by default, and requires both DNS "A" and PTR records for relay servers. If you want a RazorGate appliance to perform relaying, add the IP networks or DNS domains for which relaying should be allowed to the "Relay" list configuration. Also check DNS records for relaying hosts.

Mirapoint recommends that the relay list be kept as short as possible. You should use SMTP authentication instead of the relay list where appropriate.

DNS Blackhole List Checking

DNS blackhole list (DNSBL; also known as RBL) checking is similar to the "Reject" list but more flexible. Instead of forcing you to come up with a list of spam propagators, a pre-existing service provides a list for you. Sometimes this is a fee-based service. For more information about DNSBL services, see the Wikipedia article at http://en.wikipedia.org/wiki/DNSBL

DNSBL checking should be enabled at the point of entry to your messaging network, typically the servers that run MailHurdle.

By default DNSBL handling is set to bounce (in other words, reflect) messages. You can change handling to instead mark DNSBL-originated messages as spam by inserting a header. If you choose to insert a header, antispam scanning considers it when formulating a junk mail score. (In most situations, you should "bounce" DNSBL-originated messages.)

The DNSBL server(s) that you use should mirror your own blocking policies. Standard policies should include refusing to accept inbound mail from open relay servers and dial-up hosts.

You can set up your own DNSBL service to centralize an extensive Reject (UCE) list so it can be maintained on a single system, instead of on multiple RazorGate appliances.

Inbound Message Handling

The next security layer checks the integrity of message senders. See Figure 18 on page 47 for a flowchart of this layer.

Here is a sample SMTP session port 25, with sender interaction in bold. The MAIL FROM and RCPT TO lines constitute the message envelope.

```
220 sift.example.com MOS release
HELO yahoo.com
250 Hello, pleased to meet you mail.yahoo.com [66.218.75.184]
MAIL FROM: <joe_user@yahoo.com>
250 Sender OK
RCPT TO: <juser@example.com>
250 Recipient OK
DATA
354 Enter your message ending with "." on its own line.
Bla bla bla.
.
```

HELO Identification

Upon receiving the sender's initial HELO command and domain (or EHLO for extended SMTP) Mirapoint SMTP service checks the domain address given. If it does not match the domain address obtained by reverse DNS (see "Reverse DNS Verification" on page 20) the software could record this mismatch in the mail logs, but ordinarily does not because it is such a common occurrence. Many hosts on the Internet specify a name that is different from their DNS domain name. This could be valid domain masquerading, but nowadays is likely to be address forgery

instead. Identification is an area where security could be tightened considerably, industry-wide.

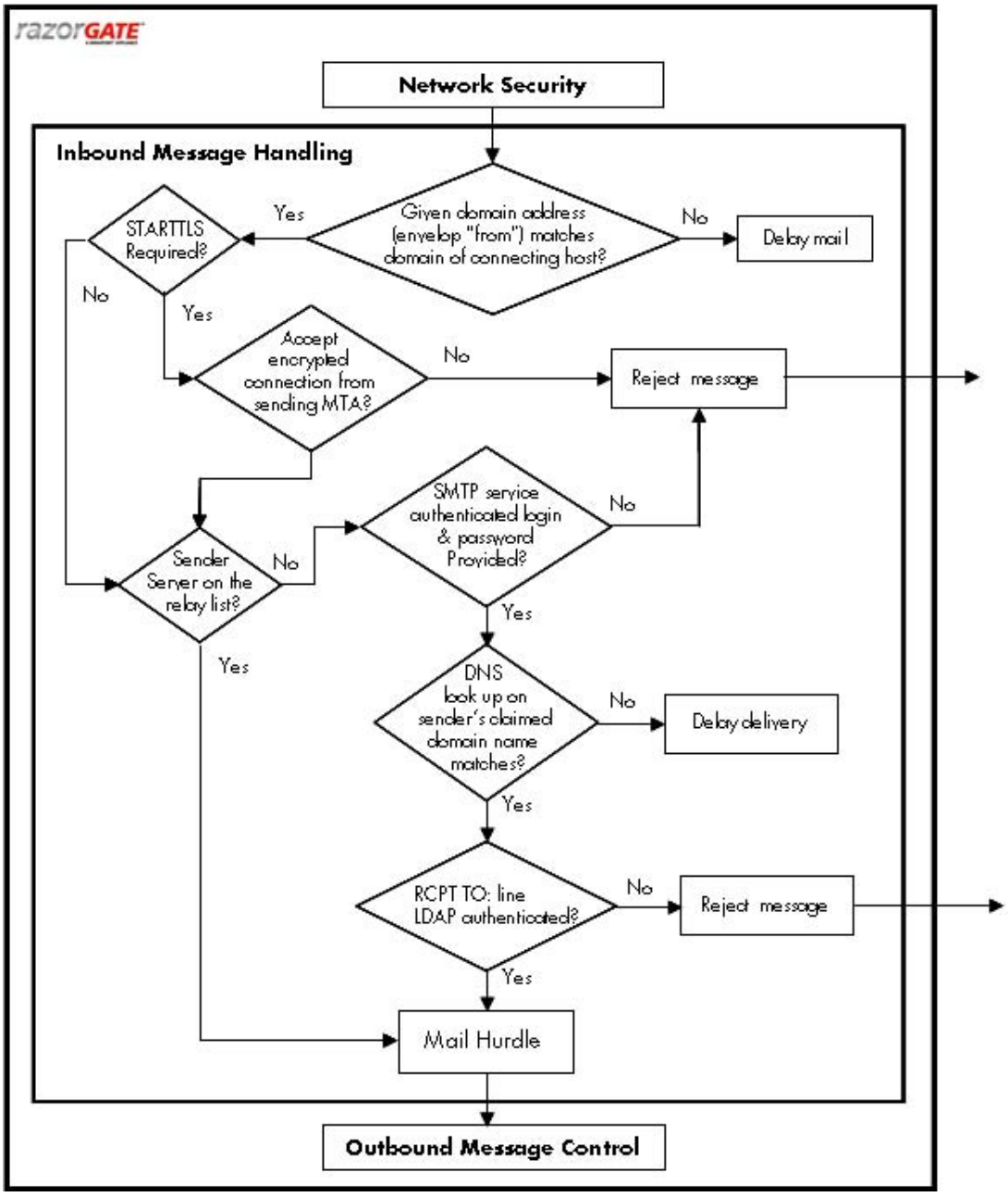

Figure 18 Inbound Message Handling Layer

SSL Encryption

Encryption makes network transmissions difficult to read for other people and software listening over the wire. With an SSL license, RazorGate appliances can be set to offer encryption for both incoming and outgoing connections. For conformance with SMTP standards, unencrypted (cleartext) connections are always allowed.

Check your RazorGate licenses to see if the system is licensed for SSL. Your Mirapoint sales representative can help you acquire a license.

Other services besides SMTP, including IMAP and WebMail, can benefit from SSL encryption. There is a performance penalty for using SSL.

When transmission security is important, use of TLS encryption is recommended. SSL and TLS encryption is recommended when users communicate with the messaging infrastructure remotely (from the Internet).Within open organizations protected by firewall, it's less of an issue. Individual messages can be encrypted using alternate methods.

SMTP Authentication

In this context, SMTP authentication means that email clients who use the AUTH command to authenticate by login and password (usually required for IMAP, POP, or WebMail connections) are also granted permission to relay SMTP messages to other hosts.

The default value for SMTP authentication is **Norelays**, which means authorization is required only when clients connect from a host not on the relay list. (The relay list should only include hosts that send mail on behalf of users that you trust, such as a local Exchange server.)

If RazorGate appliances are used to route email, many installations prefer the **Required** setting for added security.

SMTP authentication is usually strong enough. However if a RazorGate appliance is licensed for SSL, we recommend encrypting the passwords supplied for SMTP authentication.

Using SMTP authentication over a secure link is recommended for all sites. All major user clients now support SMTP authentication. SMTP authentication should be used in conjunction with sender authentication. (For more information, see User Authentication for SMTP on page 61).

Sender Check

At the next layer, SMTP service reads the MAIL FROM line, and checks validity of the originating sender's claimed domain name, if this option is on, which it is by default. It is best to accept the default, although some sites disable sender-check so they can receive messages from misconfigured senders.

```
MAIL FROM: Joe User <juser@example.com>
```

SMTP service does not ensure that the claimed domain name is the same as, or similar to, the connecting IP address, just that the domain name actually exists. This leniency was designed into email standards to allow masquerading. (For example, when an enterprise wants all outgoing email to show the same From domain, no matter from which server it originated.) Of course you can add a domain name or range of IP addresses to the Reject (UCE) list, and it will be blocked.

Leave sender-check set to its default **On** value.

Sender Address Rewrite

With LDAP masquerade enabled, the **From** address can be rewritten to match the authenticated sender, and a policy requiring that a sender be an authenticated user can be enforced to prevent outbound spamming (see Sender Normalization to Smtpauth on page 61).

Mirapoint recommends turning on Sender Address Rewrite on Outbound message servers that use SMTP auth to authenticate users.

Recipient Check

At the next layer, assuming the sender has not been blocked, SMTP service reads the RCPT TO line. If the RazorGate appliance employs LDAP authentication, or a local routing table with user addresses, it is useful to enable recipient-check. For example, the RazorGate appliance can recipient-check against Active Directory.

Recipient-check causes SMTP service to immediately reject messages addressed to unrecognized users (neither local nor LDAP), avoiding the overhead of delivery and bounce notification. Failing recipient-check creates a delay on further connections from that sender.

If the RazorGate appliance relies on an LMR (local message router) for delivery, or uses domain-based routing, recipient-check is not useful.

Recipient-check involves look-up overhead, so it is off by default. However, Mirapoint recommends using RecipientCheck wherever possible on Inbound Message Routers (IMRs).

MailHurdle

At this point the MailHurdle facility (or Mtaverify) takes effect. MailHurdle processing occurs before spam scanning, so as to reduce network load by eliminating spam up front. An illustration of how MailHurdle works is given in Figure 19 on page 50.

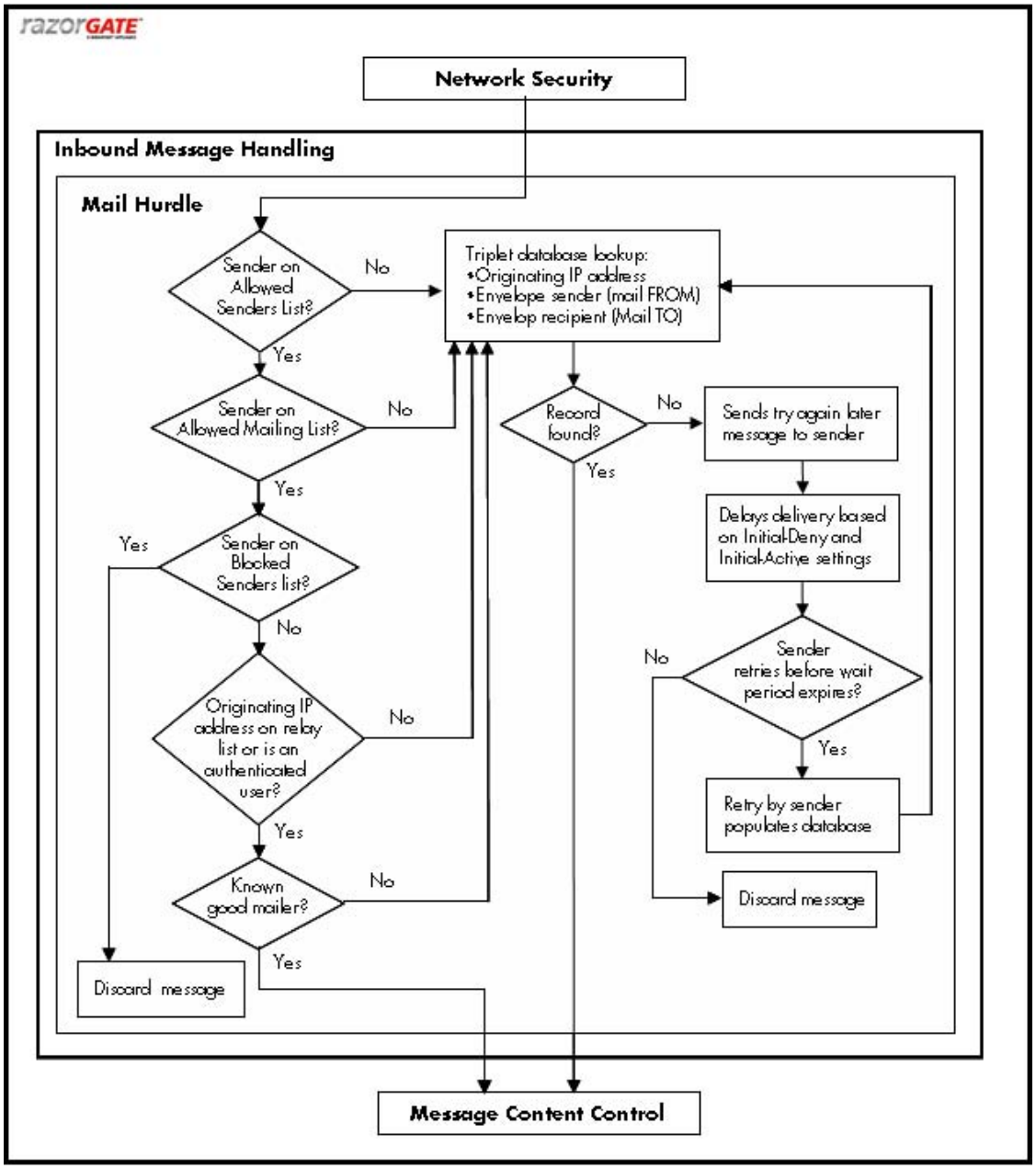

Figure 19 MailHurdle Processing for Inbound Messages

MailHurdle works by issuing a temporary failure to certain messages, requiring the sending mail server to retry sending the message. This is very effective because most spammers use quick-and-dirty mail servers, or hijacked emailers, that do not bother to retry failed messages. Legitimate mail, however, is almost always retried.

When email arrives, MailHurdle considers three items: (1) originating IP address, (2) sender address as in MAIL FROM, and (3) recipient as in RCPT TO. When messages arrive with a previously unknown combination, SMTP pretends the "mailbox is temporarily unavailable" and asks the originating server to send the message again. If this retry occurs within a certain timeframe, 5 minutes to 12 hours

by default, MailHurdle marks the combination valid, and starts accepting those messages without delay.

One deployment option is to run MailHurdle on RazorGate appliances with other security facilities such as Antivirus and Antispam scanning. A second deployment option, given high volume of incoming mail, is to run MailHurdle on dedicated RazorGate appliances and perform other security functions on a second tier of RazorGate appliances. See Chapter 2, Mirapoint Deployment Scenarios for more information.

Mirapoint recommends that MailHurdle be enabled at the point of entry into the messaging network.

On any RazorGate appliance, MailHurdle can be deployed simply by turning it on and waiting for the combination-triplet database to form. During this waiting period, messages can be delayed for a short time, depending on the retry policy of the originating message sender.

In existing installations, however, we recommend planning the transition well in advance. Formulate an allowed senders list of known-good mailers, to minimize delays in the delivery of important messages

Also determine which users (support personnel for example) should have minimal delay imposed on their email, and disable MailHurdle processing for these users.

Initial timeouts and active lifetimes can be changed from their defaults. MailHurdle can also be set to ignore the third piece of message data, the recipient(s). This reduces mail delays by only requiring a retry on the first piece of mail from a particular mail server, instead of requiring a retry on the first piece of mail from each individual sender.

Message Content Control

The next security layer examines the envelope and content of incoming messages. See Figure 20 on page 52 for a flowchart of this layer.

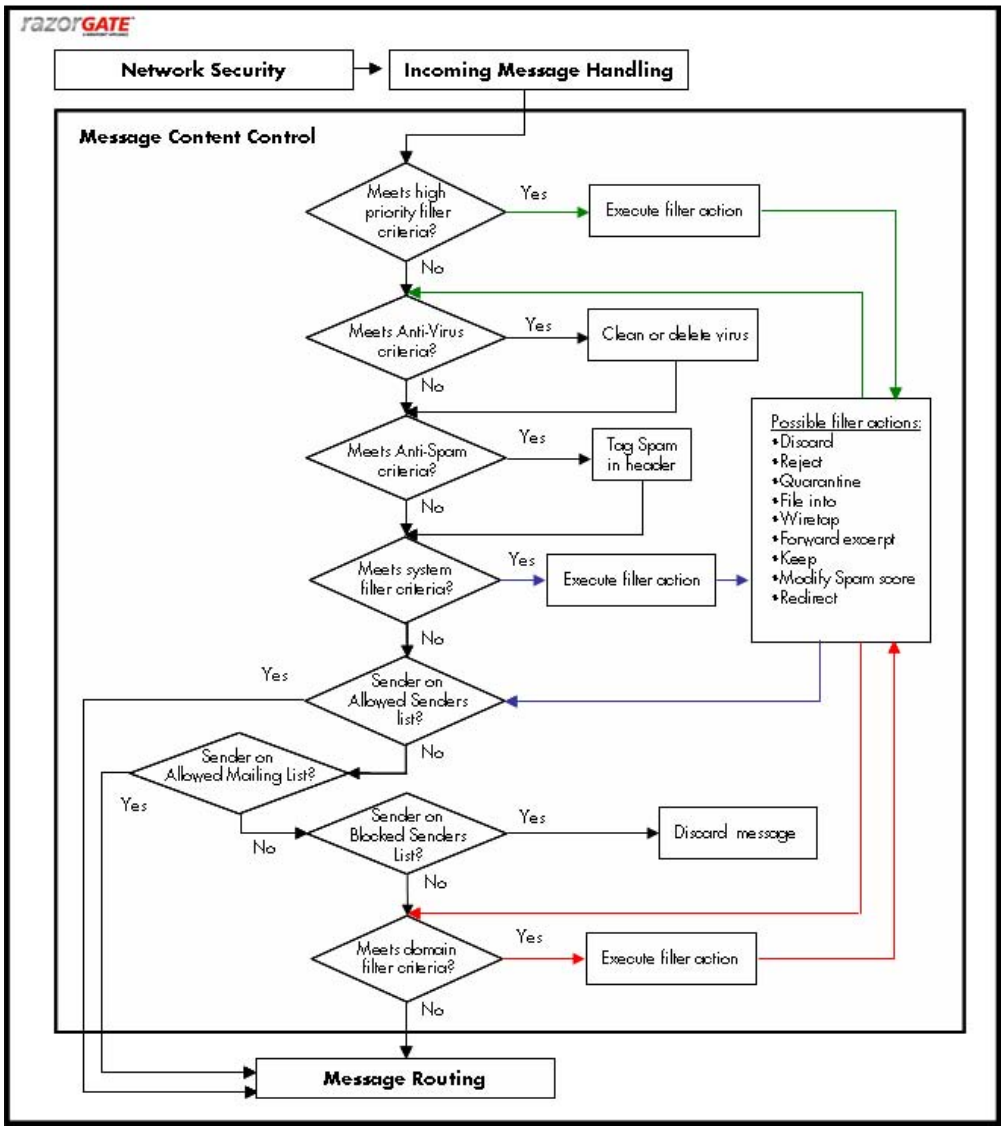

Figure 20 Message Content Control Layer

High-Priority Filters

Filters are a pattern-matching facility allowing you to recognize specific content and dispose of unwanted messages in different ways. Only administrators can create high-priority filters, which are executed before antivirus and antispam scanning. In addition to high-priority filters, there are many uses for domain-level “policy” filters; these filters are discussed shortly in Domain-Level (System) Content Policies/ Filters on page 55.

One good use of high-priority filters would be wiretap (intercept but also deliver) incoming messages from a business competitor.

Another good use of high-priority filters would be to delete attachments of certain types (EXE, VBS, ZIP) as part of corporate policy.

Before the IMR, incoming messages should seldom or never have the organization's domain name in the MAIL FROM header, for example lolita@example.com. This is a sign of a forged header. You could write a high-priority filter to bounce or quarantine all such messages.

Antivirus Scanning

Antivirus scanning is essential to protect against the threat of email borne viruses. Mirapoint offers Sophos and F-Secure signature-based antivirus scanning as well as RAPID predictive-based antivirus scanning. Which scanners you have available depends on what you have licensed.

The signature-based scanners use antivirus pattern files to recognize infected messages. By default, the Sophos or F-Secure antivirus pattern file is updated hourly at half past the hour. If you know that a virus pattern update is available sooner, you can manually update the pattern file.

RapidAV provides extra protection during the virus discovery period by identifying suspicious activity based on sending IP addresses. This identification usually takes place in 30 seconds to 2 minutes after a virus appears, providing protection in the early stages of a virus outbreak. RAPID AV does not use a pattern file but updates are required for the rulesets that it develops.

Because RAPID does not attempt to verify that potential virus outbreaks are, in fact, viruses, the only action option for RAPID AV is quarantine. An administrator with the Quarantine Administrator role, must review those messages quarantined by RAPID to make sure that they are truly viruses. An administrator can release bonafide messages from the quarantine. If no action is taken, messages are auto-released after (default) 8 hours, by which time the pattern-based antivirus scanners will have been updated.

If you want to track results of antivirus scanning, you can either enable notifications for the Virus-alerts distribution list, or look at log pages that summarize security activity for antivirus scanning.

Sender and recipient notifications were useful years ago, when people inadvertently sent infected attachments, but they are unhelpful now. Most users do not need to know which viruses are addressed to them. You can configure antivirus software to not auto-clean, which results in deletion of infected attachments.

Mirapoint strongly recommends that a signature virus-scanning engine (Sophos or F-Secure) and RapidAV are licensed on the inbound message router(s).

Antispam Scanning

Mirapoint offers two antispam products: one based on SpamAssassin open-source software, and one based on up-to-the-minute RPD (recurrent pattern detection) technology. Both are licensed drop-in solutions.

SpamAssassin identifies junk mail using heuristics, such as spoofed headers, malformed attachments, suspicious servers, type of HTML, and patterns commonly found in unsolicited bulk email. Spam traits are added cumulatively to calculate a junk mail score.

RPD is also called Rapid Antispam or Antispam Signature Edition. It consults a hash table stored on a remote website, which is maintained by a data center that quickly identifies new bulk and spam messages on the Internet. A fast hash-table lookup identifies matching junk mail.

Due to the nature of spam and the fact that spammers continually modify their attacks to circumvent heuristical analysis, Mirapoint recommends using RAPID Antispam. Antispam scanning should be done by your Inbound Message Routers.

Two downfalls of antispam scanning software are false positives (valid messages mistakenly flagged as spam) and uncaught spam (junk mail not recognized as spam) also called false negatives.

False positives are probably worse than uncaught spam, because they could lead to a breakdown in communication. Two ways to reduce false positives are upgrading to Antispam Signature Edition (RPD), which has a lower false positive rate for most users, and developing allowed senders lists. Uncaught spam can be reduced by writing content filters, or by running multiple antispam scanners in serial.

An allowed senders list is the opposite of a blocked senders list (see DNS Blackhole List Checking on page 46). Instead of rejecting messages from certain addresses, the server always delivers messages from listed addresses even if they look like spam. Administrators manage a number of system-wide allowed senders list. Users can also manage a personal allowed senders list.

Your global safe list should be kept as short as possible for maximum protection.

To keep the amount of uncaught spam to a minimum, you need to keep up with ever-changing spam techniques. Make sure that your antispam scanner is configured for frequent automatic updates.

You can schedule automatic rule-group updates at periodic intervals.
In addition to the **default** rules, Mirapoint offers **edefault** for Europe, **no8bit** for Asia, and probably others. Check a recent Support Bulletin for details.

POP users lack access to multiple folders and cannot have a separate junk mail folder, so if you support POP3 access you should configure your antispam scanner to insert “Spam” in the Subject line. That way, when users see “Spam” headers in their inbox, they can just delete them.

Domain-Level (System) Content Policies/Filters

After high-priority filters, antivirus scanning, and antispam scanning, RazorGate appliances run the domain content filters. These filters are used to enforce policies: who is allowed to do what. All filter types are implemented the same way, just executed at different stages. Filters include a selection pattern and one of the following actions. With no action, messages are delivered as usual.

- **Reject**—Do not deliver, but send bounce notification to sender
- **Discard**—Like reject, but without the bounce notification
- **Fwdexcerpt**—Forward chunk, e.g. to SMS (short message service)
- **Quarantine**—Hold message in a folder for administrator action
- **Redirect**—Alter destination address, leave message unchanged
- **Wiretap**—Surreptitiously make a copy, then deliver normally

One good use for a domain filter is to prevent outside senders from mailing to an all-employee distribution list (DL). Such a content filter checks that the "From" field contains the company domain for any messages addressed to the DL, rejecting the message if not.

Domain-level Wordlist filters are a good way to ensure that certain mail is delivered. Suppose your organization is an investment firm, and you want to continue receiving company briefs that often get classified as junk mail. You could write a Wordlist filter to deliver messages containing the string "invest" or whatever.

Mirapoint recommends placing antispam and antivirus related policies in the system content filters. Common policy choices include deleting confirmed spam if you are using RAPID Antispam and deleting infected messages if you are using a signature-based antivirus solution.

User Allowed Senders List and Blocked Senders List

After executing system-wide domain filters, RazorGate appliances consider user-level allowed senders lists and blocked senders lists before delivering email. Users set up these lists in WebMail, or by accepting a message in their daily Junk Mail Summary form.

First the software considers allowed senders lists, which are sender **From** addresses that should always be delivered. Next the software considers recipient allowed senders lists, also called mailing list exemptions, which are recipient **To** addresses that should always be delivered. Finally software considers blocked senders lists, sender **From** addresses that should never be delivered.

Users get no benefit from safelisting and blocklisting—messages are not delivered into the proper folder—until they switch the **Junk Mail Filter** from "off" to "normal" in WebMail or the Administration Suite for end-users (acctadmin). You can change user LDAP records to make this switch for them. Note that if you

implement Junk Mail Manager, this switch is not required; in fact, Junk Mail Manager requires the **Junk Mail Filter** be turned "off" (as it is by default).

Mirapoint recommends using Junk Mail Manager to manage user junk mail messages and reduce the load on the central message servers. For more information about JMM, see Junk Mail Manager (JMM) on page 59.

User Content Filters

After considering user-level allowed senders lists and blocked senders lists, RazorGate appliances execute user-level content filters. In most cases where antispam software is licensed, there is at least one content filter, the Mirapoint-preconfigured system **Junk Mail Filter** (discussed above).

The system **Junk Mail Filter** is optimized for IMAP and WebMail users with multiple folders. Users enable the filter by switching it from "off" to "normal" under WebMail **Options**, or in Administration Suite. Users set up message filters using WebMail or Administration Suite (acctadmin). Figure 21 on page 56 shows some examples of useful content filters.

Figure 21 User Content Filters

WebMail Session IDs

In WebMail and Calendar by default, the HTTP session ID is exposed in the URL. Sometimes users copy and paste their session ID into email, unintentionally giving access to their mail and schedule. To prevent this, you can set the HTTP interface to require cookies for all sessions. This is not the default, because some users believe cookies give away privacy, so they disable them in their web browsers.

For optimal internal-network security, you should require cookies for all HTTP sessions. This is configured on any host that the user connects to via the web.

Message Routing

The next security layer determines where to route and deliver messages. See Figure 22 on page 57 for a flowchart of this layer.

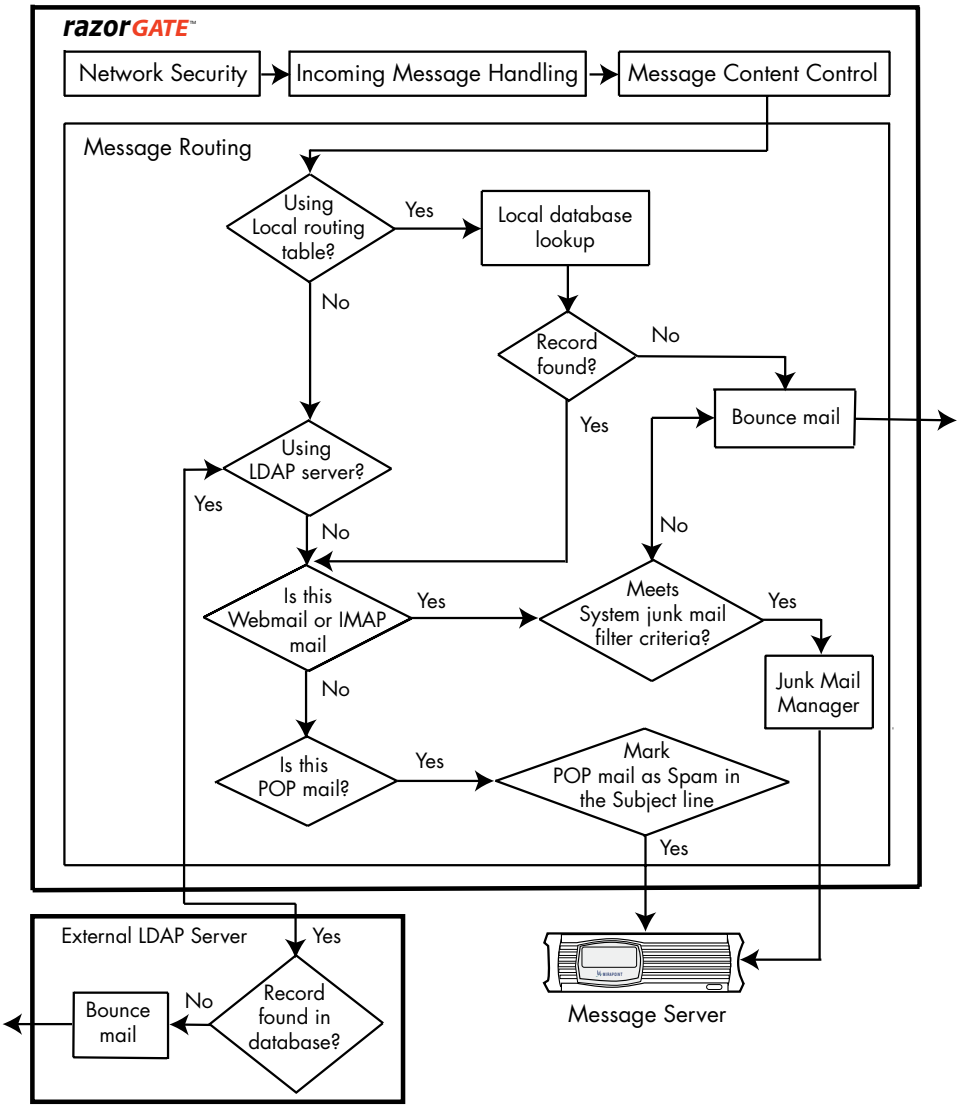

Figure 22 Message Routing Layer

LDAP Routing

A RazorGate security appliance is like a firewall, but protects your internal messaging structure, rather than specific network connections. As such, it is best to hide user and routing information on your internal network, rather than placing it on the security appliance. LDAP routing for inbound messages is one good way to accomplish this.

Among the most secure arrangements is placing a router inside the firewall, with a RazorGate security appliance inside the DMZ. The security appliance performs all

the checks described in the sections above, then the router determines destinations for message delivery.

To provide service for multiple domains, you can create a local routing table for domain-based routing. It is possible to perform individual user routing with a local routing table, but this can get cumbersome, especially for large organizations. The local routing table employs the Mirapoint internal LDAP database.

Figure 23 shows the result of specifying domain **@example.com** with the mailhost **mail.example.com**, and domain **@beispiel.de** with mailhost **post.beispiel.de** in the local routing table.

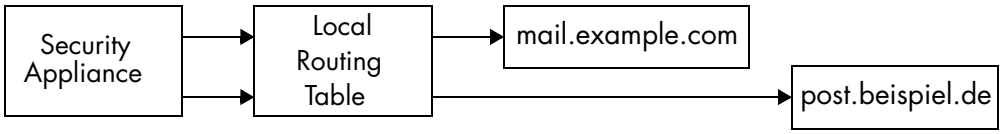

Figure 23 Domain-Based Routing with Local Routing Table

Few organizations have such clearly delineated domains as in Figure 23. Users move from one mail server to another, or are allocated randomly.

This is why large organizations often prefer to track users with LDAP. The RazorGate appliance is compatible with third party LDAP solutions, or with a Mirapoint Directory Server.

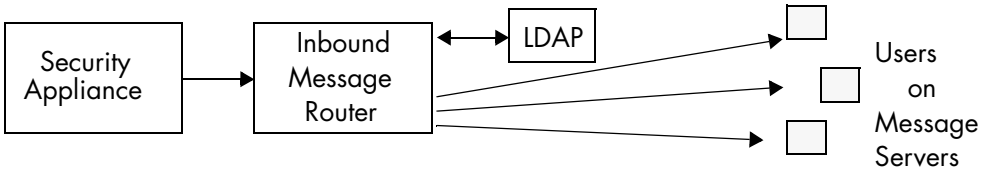

Figure 24 Routing with LDAP Database

Setting up LDAP routing as shown in Figure 24 can get complicated. You can get started by answering questions on the **Routing via LDAP** page in the RazorGate Setup Wizard.

Records in the LDAP database specify routing for individual users, based on a combination of **mail**, **mailhost**, and **mailroutingaddress**. Before users can access mail services, they authenticate themselves by entering their login and password, which must match their LDAP record. Passwords are transmitted “in the clear” (unencrypted) unless encrypted with SSL.

Mirapoint recommends using LDAP routing and SSL Security for communication between Mirapoint appliances and the LDAP server.

Junk Mail Folder

As mentioned in Domain-Level (System) Content Policies/Filters on page 55, the antispam software automatically configures the system **Junk Mail Filter** for each user. This causes messages categorized as spam (score >= 50) to be delivered to the **Junk Mail** folder. WebMail and IMAP users should be able to easily enable this feature and then find their **Junk Mail** folder.

If you implement this option, you should inform your user community that they should check their **Junk Mail** folder from time to time. Also tell users that they can optimize results by creating their own allowed senders lists, blocked senders lists, and content filters.

Mirapoint recommends using Junk Mail Manager to manage user junk mail messages For more information about JMM, see Junk Mail Manager (JMM) on page 59.

Spam in Subject (Anti-Spam Warning Flag)

POP users can see only one folder, the Inbox, so if your community includes users who lack access to WebMail or IMAP, they do not benefit from the **Junk Mail** folder. One solution for POP users is to enable Spam-in-Subject, which causes messages categorized as junk mail to have the word "Spam?" prepended to the Subject line.

Many installations also create a filter to reject messages with spam score above 299, so only messages with spam scores between 50 and 299 get spam-tagged and delivered. This risks losing email, however. Junk Mail Manager (JMM) offers a better solution for POP users.

Junk Mail Manager (JMM)

JMM is a RazorGate option that redirects spam to user quarantine folders, so it cannot clog up primary user mail folders. Users can log in to check their spam, or more conveniently, receive daily spam summaries.

In the summary, users can remotely read and/or approve any important messages. True spam is left to expire automatically. Administrators can change frequency or even disable the summary messages. For all users (POP, IMAP, or WebMail) the daily spam summary is an effective way to manage spam and avoid lost email. Table 6 shows the advantages and disadvantages of using JMM.

Table 6 Junk Mail Manager Advantages and Disadvantages

Advantages of JMM	Disadvantages of JMM
Saves bandwidth on back-end	Increased architectural complexity
Spam bothers users only once a day	Cannot blocklist users from Outlook
Users manage spam using their email	

Mirapoint recommends using Junk Mail Manager to manage user junk mail messages.

Perusing Mail and Spam Logs

To monitor security of a Mirapoint RazorGate appliance, look at the Anti-Virus, Anti-Spam, Content Filtering, and MailHurdle logs on the **Logs/Reports > Security**

page of Administration Suite. For additional more information, also check the **Logs/Reports > Mail** page.

If you notice a lot of spam originating from specific senders, add those sites, either by domain name or IP address range, to the "Reject" list or your internal DNSBL service (if available). See Network and Domain Rejection on page 45 and DNS Blackhole List Checking on page 46.

Outbound Message Control

Outbound messages from an organization use the same SMTP service as inbound messages, but security concerns are different. This section describes them in order. See Figure 25 for a flowchart.

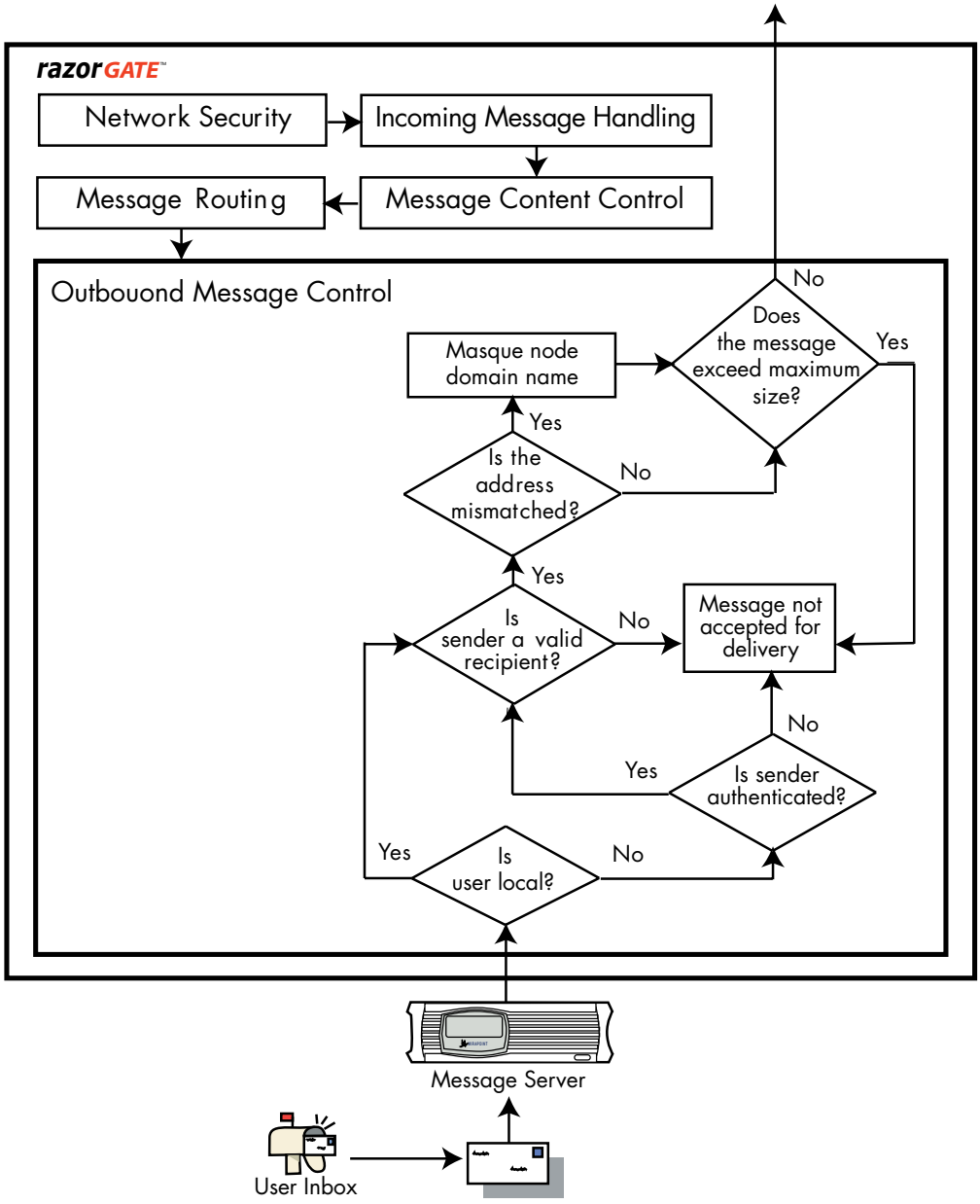

Figure 25 Outbound Message Control Layer

For most site configurations, the outbound message router (OMR) sits in the DMZ, where it has access to Internet-wide DNS, while LDAP and message servers are protected inside the firewall. You must set the OMR on all systems using it for outbound routing.

User Authentication for SMTP

The outbound router can require that users be authenticated, often by a prior mail-reading connection, before being permitted to send messages. The Mirapoint ESMTP service offers or requires AUTH LOGIN so senders supply user name and password before passing message data. This is SMTP AUTH (see SMTP Authentication on page 48).

On all outbound routers, set **Smtpauth** Required for SMTP service.

Sender Normalization to Smtpauth

Most large organizations have users scattered over multiple computers with different hostnames and possibly different domain names. Some users might transmit email from systems on totally unrelated networks. For security and compatibility, outgoing mail should always appear as if it originates from a single organization.

This is done by setting a “masquerade” for the **From** domain, the address part after @ (at-sign). Masquerade (or LDAP masquerade) normalizes the domain name. **Senderisauth** normalizes the user name.

To help avoid forged headers being sent from inside your organization, it is best to normalize user names in the **From** header to the login name supplied by SMTP authentication. This is done with **Senderisauth**.

Mirapoint recommends using SMTP Authentication over a secure SMTP link on all Outbound Message Routers.

Sender Validation by Recipient

To help avoid forged email being sent from inside your organization, some sites check to ensure that the sender is a valid recipient with **Senderisvalidrecipient** (see Recipient Check on page 49).

Although it uses the same test as Recipientcheck, we do not recommend enabling this. **Senderisauth** and **Smtpauth** accomplish the same goal.

Maximum Message Size

If network load is too high, or users complain, you can control the maximum message size that SMTP service allows. Larger messages are rejected. The default

maximum is 30 MB (31,457,280 bytes) but you can set this limit lower, or higher up to 128 MB (134,217,728 bytes).

Organizations that send lots of multimedia files by email should set this limit higher than 30 MB, perhaps as high as possible.

5

Message Store Overview

Once messages are security-screened and delivered, the message store holds them for convenient access.

In addition to core messaging services, a messaging appliance can also provide calendar scheduling, an LDAP database, backup and restore, group control, and site management.

Core messaging services for users are message storage, transfer and retrieval by various client access methods; additional services include calendaring and contact management (address book). For administrators data storage and backup, directory services, group management, system management, and various programming interfaces are supported.

Message Store

The Mirapoint message store is a hierarchical database that manages and provides access to messages in the Inbox folder and user-created folders. Messages are delivered by SMTP (see page 65) and remain in the store until deleted by user action or auto-removal. Storage is on random-access RAID for fast retrieval and reliability.

Here are the different categories of message stores:

- **Inbox**—main user folder where messages are delivered
- **Deletedmessages**—a shadow hierarchy to hold deleted messages
- **Shared**—archive mail folders that can be accessed by many users
- **Qtnbox**—quarantine folders for clients of Junk Mail Manager

To store the messages, messaging appliances must be equipped with large amounts of disk space. Saved messages accumulate over the years, so disk storage should be easily expandable.

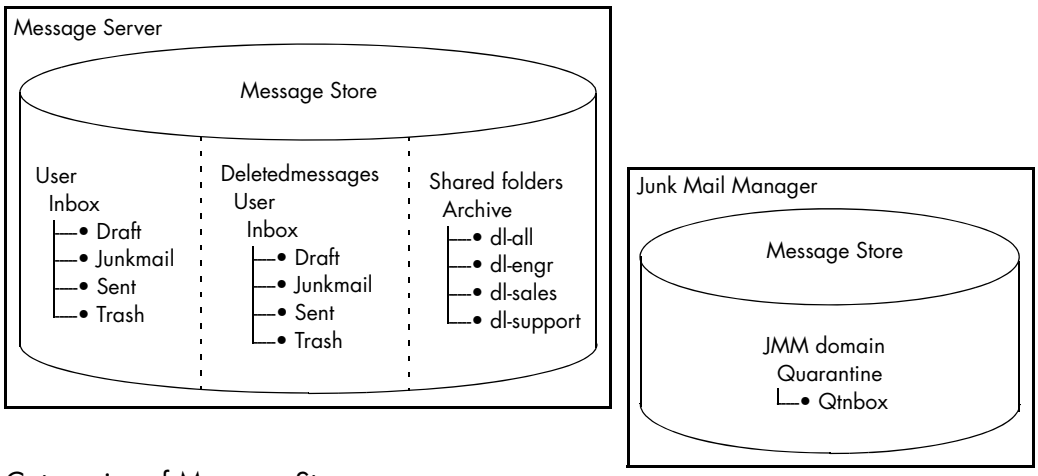

Figure 26 Categories of Message Store

On message servers, there is an Inbox for every user account. Users can create subfolders to organize their messages, if the access method supports subfolders (POP3 only allows access to the Inbox).

If an administrator enables **Msgundelete** (message-undelete facility), the Deletedmessages hierarchy (see illustration above) is automatically created when a user first deletes a message. Deleted messages and folders appear in this hierarchy at the analogous spot where deleted, and remain there (first-in, first-out) until newly deleted messages would otherwise cause the user's Deletedmessages hierarchy to exceed quota. **Msgundelete** is very useful on message servers.

Shared folders are like Inboxes, but not associated 1-to-1 with a user. Access control is set so that many users, or all users, can read messages in a shared folder. Usually shared folders are created in a separate hierarchy (such as Archive, shown above) for convenience, although users can share their own subfolders if they wish. One good use of a shared folder is to keep a record of all messages sent to a mail distribution list.

Create a mail folder each time you add a new user, or better yet, enable LDAP autoprovisioning to create users and inboxes automatically. Message-undelete is recommended, so users can conveniently find any accidentally deleted messages. If you want to provide message-undelete for selected accounts only, you can control this service using COS; see Class of Service (COS) on page 73. Shared folders can be published (made accessible) over multiple systems using special LDAP schema, called 3TSF (three-tier shared folders).

JMM Quarantine

Quarantine folders (Qtnbox) replace the Inbox on Junk Mail Manager (JMM) systems. JMM initially sets auto-expiration to 14 days on the Qtnbox. Note: JMM must run on a separate system from the message store.

Message Transfer

These include SMTP for delivery, IMAP and POP for standards-based message access, and WebMail for browser-based message access.

Simple Mail Transfer Protocol (SMTP)

SMTP (simple mail transfer protocol) receives messages from other hosts and inserts them into the message store. In a multi-tier setup, the security appliance and inbound router perform screening and routing operations, so SMTP on messaging appliances has a relatively simple delivery function. On the outbound router, SMTP delivers messages from local users to addresses on remote hosts across the Internet.

After software installation, SMTP is disabled by default, to avoid sending any unwanted email, and to prevent misdelivery of messages addressed to users on the new server.

After correct DNS configuration of MX and possibly CNAME records, enable and start SMTP service on every Mirapoint appliance. Visit the **System > Services > SMTP** pages in Administration Suite, or check **Smtp** command settings in the CLI, to customize service configuration.

Internet Message Access Protocol (IMAP)

IMAP (Internet message access protocol) is a message access protocol that allows the user to centrally access and manage their messages from a desktop client such as Microsoft Outlook or Mozilla Thunderbird. Each user has a main folder (Inbox) on a server, where SMTP service usually delivers email. IMAP users can create their own subfolders, and set access permissions separately on any of their folders. Multiple users can simultaneously access a subfolder, if access permissions allow.

IMAP is very convenient and flexible for users and allows for a centralized data retention and backup policy. However, this convenience comes at cost. Most sites find they can support at least 10 times more POP users than IMAP users on a given appliance. It is possible to provide IMAP service to some users, and only POP or WebMail to others, by creating different classes of service with the COS facility. IMAP service should be enabled on message servers, but is not needed on security appliances.

Mirapoint recommends that enterprises offer WebMail and IMAP to users to provide centralized policy controls and backup.

Post Office Protocol (POP)

POP (post office protocol) is a service that lets users download their messages from a server to a desktop client. After download, messages are removed from the server, but available on the desktop client. Unlike the IMAP service, POP users only access their Inbox folders. Message organization is done within the desktop client.

POP is an efficient protocol, but provides minimal functionality aside from reliable message delivery. Because POP does not allow subfolders, it is impossible for an

antispam scanner to divert spam into a Junk Mail folder where users can mostly ignore it. This is why Junk Mail Manager is extremely helpful for POP users.

WebMail

WebMail is a Mirapoint service that allows users to access and manage their messages directly. Each user has a main folder (Inbox) on a server, where SMTP service delivers messages. Users can create subfolders, and set access permissions on any of their subfolders. Multiple users can access shared folders simultaneously.

WebMail allows users to:

- Access messages delivered to their inbox
- Compose messages, check spelling, and send messages
- Create and delete subfolders to help manage email
- Store contact addresses and groups, with import and export
- Control folder access by creating an access control list (ACL)
- Create message filters for inboxes, including blocked-sender lists
- Set automatic reply or forwarding for messages

Use of a standard web browser instead of a specialized application eliminates the need to configure IMAP or POP clients on every user's computer, and permits easier roving access. Users can log in and easily read their email from any Internet cafe anywhere.

Mirapoint offers two different WebMail solutions: standard edition and corporate edition. A comparison of the supported features is shown in Table 7.

Table 7 WebMail Features Comparison

Features	WebMail Standard Edition	WebMail Corporate Edition
Mail Access and Management	Yes	Yes
Integrated Address Book	Yes	Yes
Personal Calendaring	Yes	No
Group Calendaring	Yes	Yes
Enhanced User Interface	No	Yes
AJAX Support	No	Yes
Branding Options	Fully Customizable	Themes, links, and logos
Target Audience	Service Provider	Enterprise

Mirapoint recommends deploying WebMail for remote or mobile users when IMAP is also deployed.

Deleted Messages

Users frequently delete messages by accident. Many email clients, including WebMail, have a "delete to Trash" option. In WebMail with this option enabled, messages stay in the **Trash** folder until emptied.

As an alternative, you can offer message-undelete to all users, by setting a folder **Undeletequota** for everyone. By subscribing to their **Deleted Messages** folder, users can move (drag and drop) deleted messages back to their regular folders. When users delete so many messages as to exceed the undelete quota, older deleted messages are purged, in order, until their **Deleted Messages** folder is 10% below quota.

Needless to say, offering message-undelete to everyone requires a lot of disk space. A better alternative might be offering message-undelete to selected users only. You can arrange this by enabling **Msgundelete** in COS, and placing the **miMailUndeleteQuota** attribute, optionally with different values, in selected user LDAP records.

Mirapoint recommends that all users get a small message undelete area. Undelete reduces the need for folder restorations since users generally realize immediately that they mistakenly deleted something.

Shared Folders

Just by changing the ACL (access control list), it is simple to set up shared folders on a single server. Most administrators put shared folders in a special hierarchy named **archive** or something similar, to make shared folders easy to find.

Mirapoint also offers the 3TSF (three-tier shared folders) facility to enable multiple servers to serve the same group of shared folders. This means that users don't need to switch servers to subscribe to a shared folder on a different server. (Without 3TSF, users on a different server must switch servers and subscribe to access a shared folder on that server.) 3TSF requires special Mirapoint LDAP schema and query settings. (3TSF is only applicable in a multi-tier deployment with multiple mail stores.)

Quarantine

In messaging, a quarantine is a safe area to hold messages for a time before delivery or disposal. Mirapoint appliances have many different types of quarantine folders. In delivery order they are:

- RapidAV jail—Messages that are suspected of carrying a virus that has not already been detected by a signature virus scanner are held in the RapidAV jail for up to 8 hours. On release, they are re-submitted to the signature virus scanner.
- Antivirus quarantine—Messages containing confirmed live viruses are held in the antivirus quarantine. A quarantine administrator will periodically review messages to ensure that no important message is caught. Messages should never be released from the quarantine (they contain live viruses), but other actions

can be taken, such as informing the recipient of the message or requesting a virus-free re-transmission.

- Filter quarantine—Messages containing words or phrases in the corporate or objectionable word list can be sent to the filter quarantine. These messages can then be reviewed by a quarantine administrator (normally someone within Human Resources) and either released or rejected.
- JMM quarantine—Messages identified as spam can be directed to a personal JMM folder. End users can control the release of messages from the JMM quarantine for delivery to their normal Inbox. Messages not released are automatically expired after a period of time.

Encryption

To promote data privacy and security, Mirapoint appliances provide data encryption for various connection types. Certificate-based server authentication is also provided to establish trust.

- SSL (secure sockets layer)—SSL is a data encryption protocol that is licensed from Mirapoint. Normally, strong encryption that uses 128-bit SSL is licensed. In certain cases (usually due to US trade restrictions on encryption technologies), only 40-bit (weak) encryption will be available.

  SSL encryption is available for the following types of connections: secure administration protocol (adminds), secure HTTP (https), secure IMAP (imaps), LDAP over SSL (ldaps), secure POP (pop3s), and WebMail or WebCal in secure mode (using https). SMTP uses TLS, a similar encryption technology to SSL that uses the same keys.
- A SSH (secure shell) license, usually bundled with SSL, enables secure connections to the CLI using the Linux **ssh** application or equivalent. When any security license is applied to the system, the Administrator can also access the administrative CLI via SSH (secure shell).

Mirapoint recommends securing your messaging infrastructure using strong encryption. To prevent pop-up screens for the end-users, the SSL certificate should be obtained from a recognized certification authority such as Verisign.

User Proxy

When there is only one message server, users can be instructed to log into the server directly to access messages and send mail. However, when multiple mail stores are used, a proxy layer is recommended so that you have a single login point for all users. Users log into the proxy server and the proxy performs an LDAP lookup to locate the correct mail store and silently transfers data to that mail store. This simplifies support and enables administrators to move users between mail stores to balance the load without impacting users.

Often an inbound or outbound message router doubles as the connection proxy.

Mirapoint recommends designating a user proxy when more than one mail store is used. This function can be combined with the Outbound Message Router in smaller environments or split off into a separate tier.

HyperText Transfer Protocol (HTTP)

Mirapoint appliances include an HTTP server to provide access for WebMail standard edition, WebMail corporate edition, calendar or group calendar scheduling, Administration Suite, and HTML online help. The HTTP proxy functions just like the IMAP and POP proxies described above.

Calendar

Mirapoint offers several calendaring solutions: WebCal for personal scheduling, and GroupCal for coordinating with other people's schedules in an organization. WebMail standard edition might show a link to personal or group calendar, whichever is licensed. WebMail corporate edition integrates group calendaring into the same application as email, providing the same functionality as GroupCal.

Calendar information is associated with user accounts. Optionally, calendar information can be synchronized with the Outlook calendar; see Outlook SynQ on page 70.

Mirapoint recommends using group calendaring in conjunction with Mirapoint WebMail or IMAP messaging deployments for a complete messaging environment.

WebCal Personal Calendar

The WebCal service lets users establish and retrieve personal calendar appointments using a web browser. Users can do the following:

- Access their calendar with a weekly, daily, or monthly view
- Create events with automatic event notifications
- Create a to-do list
- Store contact address information, with import and export

Calendar appointment reminders are sent by email shortly before the engagement, and optionally in the early morning hours.

WebCal Group Calendar

With addition of the GroupCal license, users can also do the following:

- View other users' calendars (depending on permissions)
- Suggest and schedule meetings with other users
- Accept or decline calendar appointments from others
- Exclusively book shared resources such as conference rooms

Outlook SynQ

Outlook SynQ is a product that synchronizes data between an Outlook email client and a Mirapoint calendar server. It harmonizes the following items: calendar events, calendar attachments, address book entries, and items on the to-do list.

Address Book

The address book provided with WebMail is also used by WebCal and GroupCal. To assist with scheduling, users can record information about people in their contact list, including address, company, several phone numbers, personal notes, birthday, and anniversary date.

Personal contact information is associated with a user's account. Users can import and export address-book data in various formats, such as LDAP interchange format and CSV (comma-separated values).

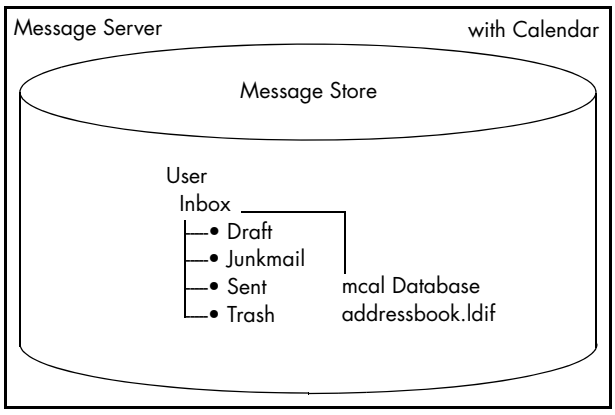

Figure 27 WebCal, GroupCal, and Address Book

A well-specified LDAP database can include address-book contact information for all users in the organization. You can make this data available to the WebMail and WebCal address book. Users can add other contacts to their personal address books.

Mirapoint recommends that enterprises with a corporate directory (for example, Active Directory) add this as a globally available corporate address book to the WebMail system.

Storage and Backup

Mirapoint always builds redundancy into power supplies, cooling fans, network interfaces, and disk-storage subsystems.

Redundant Array of Independent Disks (RAID)

Many Mirapoint appliances are designed with internal RAID storage, or an external RAID disk shelf. Some configurations use simple RAID-1 mirroring, while others employ cooperating RAID-5 or RAID-10. All RAID storage can tolerate the

failure of one disk drive, sometimes with reduced performance. For arrays larger than RAID-1, the missing disk information is extrapolated from block parity on remaining disks.

Addition of a “hot spare” disk allows substitution of the hot spare for the first failed disk, so appliances can tolerate two disk failures before an operator must replace disk drives.

On appliances with important static data, including message servers, routers with long mail queues, and LDAP servers, Mirapoint provides a hot spare for every RAID array. If any disk in the RAID fails, replace it as soon as possible. Security appliances have less stringent redundancy requirements, but they are best deployed in pairs so one can take over if the other fails.

Network Attached Storage (NAS)

Certain Mirapoint appliances store data on network attached storage (NAS). You might choose this option instead of RAID storage if you have existing NAS servers, or want to share data with other facilities. Contact your Mirapoint sales representative for more information.

Storage Area Network (SAN)

Certain Mirapoint appliances store data on a storage area network (SAN). You might choose a SAN solution to centralize storage for many Mirapoint appliances on a single device, instead of having separate RAID disk shelves for each appliance, or to accelerate data backup. Contact your Mirapoint sales representative for more information.

Failover and Cluster

In a failover configuration, a secondary head unit (with processor and memory) can take the place of the primary head unit in case of failure. Both head units are connected to the same RAID storage subsystem, so data integrity is maintained after failure.

In a cluster configuration, one head unit can take the place of any active head unit in case that unit fails. You can deploy up to nine active head units in a cluster.

A failover configuration requires either SAN or Mirapoint RAID storage. Cluster failover requires SAN.

Backup and Restore

Mirapoint supports these backup solutions:

- Veritas NetBackup Network Data Management Protocol (NDMP)
- Legato NetWorker using NDMP
- Tivoli Storage Manager using NDMP
- BakBone NetVault using NDMP

Mirapoint does not back up SAN and NAS storage. You need to use the storage vendor's backup procedures.

Mirapoint recommends the use of NDMP image backups for disaster recovery purposes when using Mirapoint RAID storage. The backup schedule will be driven by your organization's needs.

Directory Services (Account Management)

If you have an all-in-one Mirapoint appliance, it might be acceptable to store all user-account data locally. But as soon as you add a second messaging appliance, you'll want to access user-account data from the new appliance. If you deploy multiple appliances from the beginning, for instance a RazorGate appliance for security screening and routing, plus a Mirapoint message-store appliance for serving messages, the advantages of centralized user-account data are immediately obvious.

Lightweight Data Access Protocol (LDAP) is the standard choice for storing user-account data, although there are alternatives (see Network Information Service (NIS) on page 73). On Mirapoint appliances, LDAP assists message routing, user authentication, account quotas, service levels, interface preferences, and other features. Other methods for storing user account data only store authentication information.

Mirapoint Directory Server

All Mirapoint systems contain an internal LDAP server, managed by the **Dir** service. This is a fully functional directory server with relatively high performance implementing LDAP v3. Data can be written to and read from the local LDAP server, but without a license, other systems may neither read nor write data on that LDAP server.

To make LDAP information available for queries by other systems, a Directory Server license is required. In multi-tier installations, LDAP information is often placed on the same appliance as user mail folders, and later moved to a separate system for higher performance.

The Mirapoint Directory Server supports replication. To help improve reliability, the LDAP database can be mirrored on a second appliance. LDAP queries go to the second server if the first is unavailable.

LDAP Autoprovisioning

A major advantage of LDAP is that, once you have created user records in the database, accounts are automatically created on message servers when email arrives or users login. No administrator action is required.

As of release 3.8.0, user-spam accounts on Junk Mail Manager (JMM) may also be autoprovisioned.

To autoprovision accounts, the Mirapoint appliance must be able to find the mail address (or published name), login ID, and mail host of the user. Other LDAP

attributes are used to specify mail account settings (such as mail quota, alternate email addresses, and class of service), webmail preferences, and group affiliation.

LDAP Schema Extensions

Mirapoint Directory Server comes with six prepackaged schema, four of which (core, cosine, inetorgperson, and misc) are standard. However the **mirapoint** and **mgrp** schema are Mirapoint specific, and (especially the former) might change from release to release.

If your site uses Mirapoint Directory Server as your LDAP database, upgrading system software also updates the Mirapoint-specific schema.

If your site uses a third-party LDAP server, Mirapoint strongly recommends adding the **mirapoint** and **mgrp** schema to your LDAP server, and updating them every time you upgrade Mirapoint system software. Failure to do so could mean that certain operations may fail (for example, when webmail preferences are stored in LDAP, failure to update the schema could result in the inability for users to change their webmail preferences).

Class of Service (COS)

Class of Service (COS) is a Mirapoint facility that can allow or deny user access to certain system services. You could use it, for example, to allow IMAP access for certain users, but not for other users. IMAP is more resource-intensive than POP or WebMail. Currently 21 different messaging services are under COS control.

COS requires an LDAP directory server with custom Mirapoint schema, in particular object class definitions for **miCosDn**. Additionally, user records in LDAP should contain allowed COS services, or preferably, the miCosDn attribute referring to a named class of service.

Service providers employ COS to provide different grades of service, perhaps at different cost. For example, bronze service might provide POP access and antivirus, silver service might also provide WebMail and antispam, while gold service might also provide IMAP and optional data encryption with no quotas.

Mirapoint recommends using LDAP for user management.

Network Information Service (NIS)

Network Information Service (NIS) on Mirapoint appliances employs a remote NIS or NIS+ server, often a Sun system, to authenticate user logins and store a limited amount of user account information. This service is sometimes called Yellow Pages. For details, see the CLI online help topic **Help About Nis**. Nowadays LDAP has mostly replaced NIS.

Remote Authentication Dial-In User Service (RADIUS)

Remote authentication dial-in user service (RADIUS) is an authentication, authorization and accounting protocol. Mirapoint supports RADIUS

authentication for login verification of users. A Radius server must exist on the network.

RADIUS is most often used by service providers and generally provides a gateway to other authentication techniques, such as SQL.

Group Management

Group management is handled through delegated domains, distribution lists, and LDAP groups.

Delegated Domains

The Mirapoint delegated domain facility duplicates the function of real DNS domains. A single appliance can serve many domain names, with users grouped into delegated domains, all receiving messages and logging into accounts in that domain. For example, an ISP example.net could offer full-scale Internet services to joesdiner.com and wbay.com, among others, served from the same appliance. All employees of Wbay could have email addresses like fred@wbay.com, and they wouldn't even have to know that example.net is their ISP.

The reason these domains are called "delegated" is that, with a license, the top-level administrator of example.net can delegate administrative responsibilities to a domain administrator for each delegated domain served by the ISP's Mirapoint appliances.

All delegated domains created on a Mirapoint appliance should have an MX record in DNS, and optionally an "A" or CNAME record too.

Distribution Lists

A distribution list (DL) is a named set of Mirapoint users grouped under a single address. Messages sent to the DL are delivered to all.

For instance, all employees in a company's marketing group could be added to the dl-mktg@example.com address. Sending email to the DL is more convenient than addressing everyone individually.

You might also want to create shared folders for important DLs to facilitate future access and backup. The shared folder can be added to the DL, just like a member address, but preceded by a plus sign, for example: +archive.dl-all@example.com.

LDAP Groups

Distribution lists are local, so in multi-tier installations, they are usually replaced by LDAP groups. These have the same function as a DL, but are maintained in the LDAP database to make them available site-wide.
As defined in the Mirapoint **mgrp LDAP** schema, the object class is mailGroup, and involves the attribute types mgrpRfc822mailMember, uniqueMember, and Owner.

System and Site Management

System and site management is handled through the CLI (command line interface), the Administration Suite web-based interface, and the Operations Console interface. Additionally, Mirapoint supports read access and notifications using SNMP traps.

Command Line Interface

Administrators can telnet to a Mirapoint or RazorGate appliance to manage messaging using the administration command-line interface (CLI). This interface offers many commands and options, so online help is provided.

Conceptual introductions are available with **Help About**. Commands and options are documented by **Help *Command*** write-ups. The Tab key completes commands and shows what subcommands are available at your current location. The up-Arrow key repeats commands in the history list. The left and right Arrow may be used to edit a command.

Administration Suite

Using any standard web browser, administrators can access the graphical user interface (GUI) of Administration Suite to manage messaging appliances. The Administration Suite is not as functionally complete as the CLI, but can more easily manage all important aspects of a Mirapoint Message Server or RazorGate appliance.

Mail folder owners can access a small subset of the Administration Suite (acctadmin) to control their account settings if they do not have access to WebMail options.

Administration Protocol

With any programming language that supports TCP/IP sockets, administrators can write custom scripts using the Mirapoint administration protocol. For more information, see Administration Protocol on page 77.

Mirapoint Operations Console (MOC)

The Mirapoint Operations Console (MOC or OC) is a good way to manage groups of appliances, especially when multiple appliances have the same configuration. You can use MOC to manage groups of servers, assign a master server, and replicate configuration within group.

The main **Dashboard** page shows all groups, the hosts in each group, the IP address of these hosts, the MOS version, and overall status.
The **Import/Export** page allows you to write out and read in the configuration data for managed appliances.

For all monitored hosts, the **Alerts** page shows the name of an alert, a description of it, and the length of time since the alert began.

MOC has three default groups: Inbound Routers, Outbound Routers, and Security Layer. You can click **Edit** to create more groups, and to add members, including the master, to existing groups.

Mirapoint Messaging Reporter (MMR)

The Mirapoint Messaging Reporter (MMR) is a Microsoft Windows application that lets administrators manage email security information and events. MMR automatically collects device log files, normalizes data across disparate devices, and aggregates all this data into a database. MMR then correlates the data for monitoring, alerting, reporting, and forensic tasks.

Figure 28 shows the a typical MMR control window.

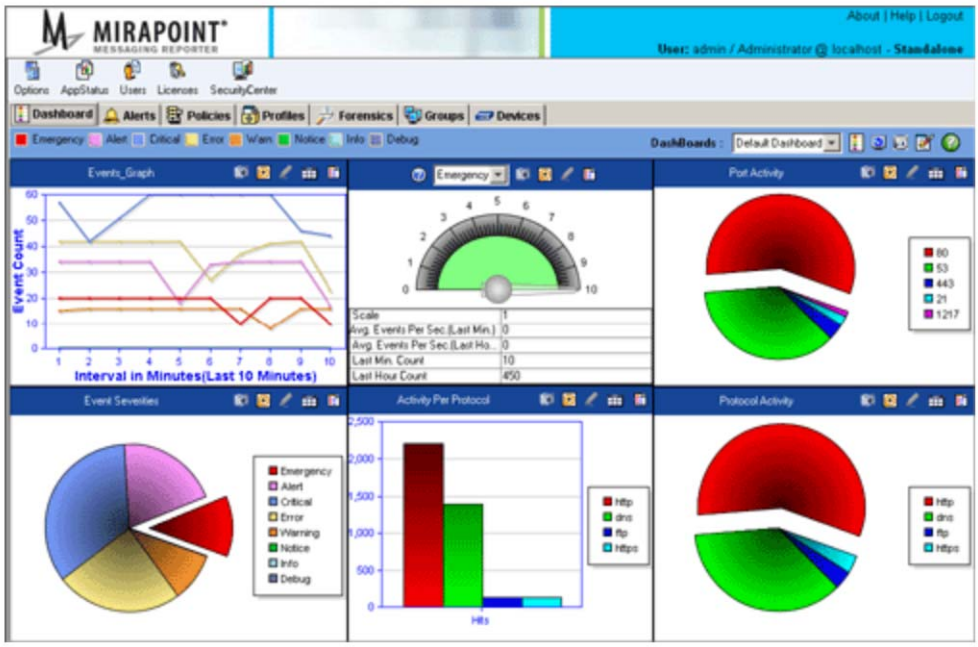

Figure 28 Mirapoint Messaging Reporter (MMR)

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) service allows consoles to centrally monitor selected information about Mirapoint appliances. SNMP consoles are available from a multiplicity of vendors, and can monitor many other systems besides Mirapoint. Most SNMP products have graphical interfaces where administrators can select items to monitor, and drill down for specific information.

Mirapoint supports read access and notifications using SNMP traps. Write access is not permitted. A management information base (MIB) is downloadable from any Mirapoint host. For download instructions, see **Help About Snmp** in the CLI.

Programming Interfaces

Mirapoint customers can employ various programming interfaces (C, Perl, Java) for the following purposes:

- Writing internal software interfaces
- Initiating system migrations, both in and out
- Portal and application integration
- Reporting, monitoring, and provisioning
- Third-party partner integrations

Administration Protocol

Using the Mirapoint administration protocol, you can write software to perform batch administration tasks on a Mirapoint system locally or over a network. Unlike the CLI, which is optimized for interactive use, the low-level administration protocol was designed so programmers can automate administrative tasks using scripts.

Examples of administrative tasks include: creating and deleting users, managing quotas, and producing usage reports. The protocol supports the implementation of more ambitious applications, such as complete provisioning systems, report generation tools, complex distribution list management systems, or automated help-desk attendants.

Mirapoint Administration with Perl

Perl has become a popular programming language for writing system administration scripts. It can be readily used to automate Mirapoint administration. Mirapoint provides a Perl library called **Net::MirapointAdmin** for administering messaging systems. For details refer to the "Automating Administration with Perl" appendix of the *Mirapoint Administration Protocol Reference*.

XML/HTTP Interface

Mirapoint's calendar, address book and message store can be accessed through a feature-rich XML/HTTP interface, allowing alternate interfaces (such as mobility solutions) to be developed. The XML interface is a licensable feature.

The interface can also be used to synchronize Mirapoint calendar and address data with other applications.

The interface provides functions to retrieve, add, modify, and delete messages, calendar events, and contacts. You can import and export calendar data in vCalendar format and address book data in LDIF format. Message data can be accessed without worrying about the encodings and the interface can also be used to send email through Mirapoint systems.

The XML group calendar interface can also retrieve events and to-do items, get to-do items, get events within a given date range, search for events and to-do items,

import and export vCalendar data, set and get user preferences, check for changes to records, subscribe to other calendars, view other users' calendars, and get free/busy data for any user.

Glossary

A

Mirapoint-specific terms in this book are defined as they are used. Important industry-standard terms are defined in Table 8.

For more information about messaging terminology and concepts, refer to the Wikipedia email article at http://en.wikipedia.org/wiki/Email or one of the many other Web resources, such as Foldoc.

Table 8 Glossary of Important Network and Messaging Terms

Term	Meaning
authentication	The way in which user data is validated. Mirapoint systems support several authentication methods, including LDAP, Kerberos, and plaintext.
distribution list (DL)	A named list of email addresses (user accounts with folders). When you send a message to a DL, the message is sent to all the addresses on the list.
DNS	A common method used for establishing Internet addresses so mail can reach its correct system destination. An example of a domain name (not including host name) is example.com. A sample user email address is whozit@example.com.
DNS domain name	The DNS domain name of a network, for instance, example.net. Domain names are case-insensitive.
envelope	The portion of a message that contains machine-readable information that helps email systems deliver the message.
fully qualified domain name (FQDN)	A complete system name that includes the names of a host, possible subnets, organization domain, and the top-level domain name. For example, k9.eng.example.com is fully qualified, whereas k9.eng is not.
host name	A name given to your Mirapoint system (such as mail1), not including the domain name. Host names are case-insensitive.
HTTP (HyperText Transfer Protocol)	The client-server TCP/IP protocol used on the World-Wide Web for the exchange of HTML documents. It conventionally uses port 80.
IMAP (Internet Message Access Protocol)	Networking protocol used for retrieving and managing email messages, passed between a message server and its clients.

Table 8 Glossary of Important Network and Messaging Terms

Term	Meaning
IP address	The Internet Protocol (IP) address assigned to a system, including your Mirapoint box, expressed in dotted-quad notation (such as 192.168.0.28).
LDAP (Lightweight Directory Access Protocol)	A networking protocol that allows for remote database search and retrieval of information. Mirapoint systems use LDAP for authentication, routing, and proxying.
masquerade	A DNS domain appended to all unqualified addresses in message headers—addresses not containing the at sign ("@"). If a relay host is specified, masquerade affects message headers.
MIME (Multipurpose Internet Mail Extensions)	A protocol that allows you to incorporate multimedia attachments to email messages. These include still images, movie clips, sound files, binaries, and text files.
MX record (Mail Exchange record)	A DNS resource record indicating which message server handles email for a given domain. The host is specified as a name, not an IP address. The primary mail server is assigned a high preference level, while backup mail servers are assigned medium and low preference levels.
NTP (Network Time Protocol)	A protocol built on top of TCP/IP that assures accurate local timekeeping with reference to radio, atomic or other clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
POP (Post Office Protocol)	A service that lets users retrieve their email messages. Unlike the IMAP service, the POP service does not allow access to multiple folders; users can access only their own Inboxes.
port	A number used to identify a service on a computer. This number distinguishes the service from other services running on that computer.
proxy	One entity acting for another, for example a web caching proxy or a firewall security proxy. In the Mirapoint context, a message switch acts as a proxy for message servers. This allows distribution of user folders among multiple message servers while hiding the details of which message server was used.
relay	The act of passing along messages to another server.
router	The machine deciding folder location for delivery. Note: Email routers are sometimes known as relays.
SMTP (Simple Mail Transfer Protocol)	Protocol used by the delivery service that receives email for delivery to local folders and transmits outgoing email to other computers.

Index

N

O

P

Q

R

S

T

U