



Technology Transfer Partners

GroupWise SMTP Infrastructure Design:

GWIA configuration and use

Lawrence Kearney
Advisory Board Member and Representative
for Higher Education in the Americas

lawrence.kearney@earthlink.net
<http://www.lawrencekearney.com>

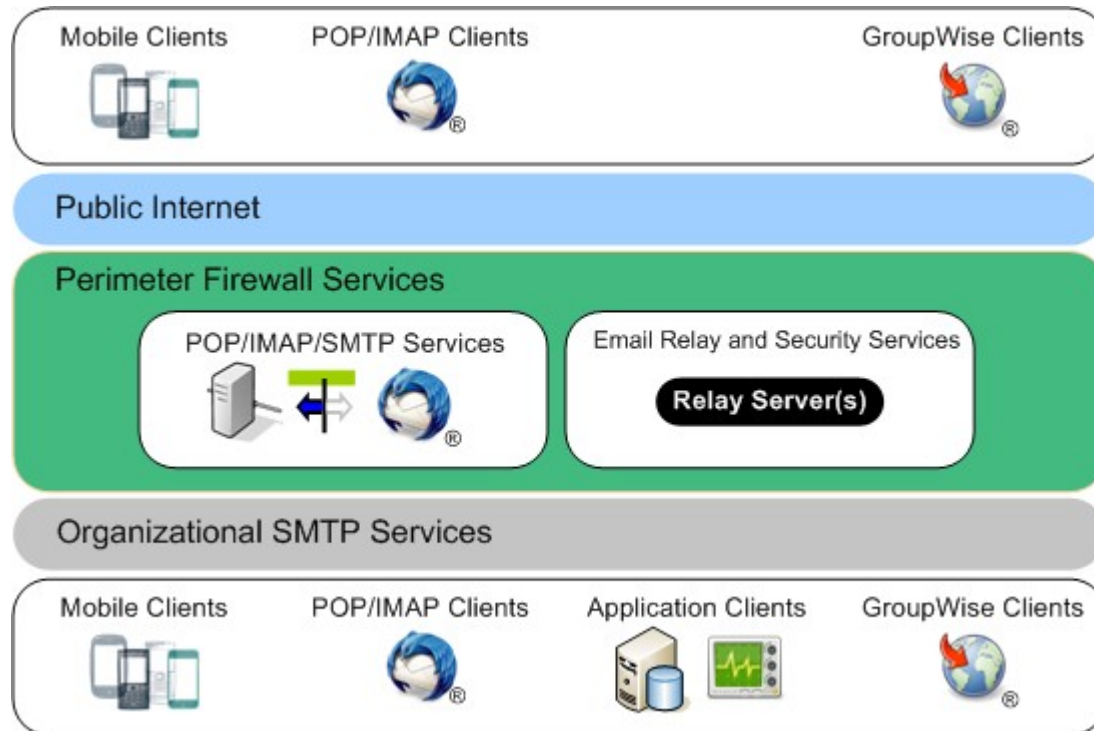
Focus on the technical aspects of design, deployment and configuration

Most information applies to large and enterprise size environments

Designing systems to compete with similar commercial service offerings

Maximizing value using basic infrastructure resources

Services normally compete for system resources



How well a service does when measured ...

Performance

Stability

Features

Cost of ownership

Scaling

Security

Separate different messaging workloads

Current messaging service needs are more complex

Assessing complexities helps identify design solutions

Updating legacy design keeps on-premises systems viable



- Clever architecture and design choices
- Service I/O demarcations (QoS really)
- Service load balancing/management
- Application redirection/fail over
- Service high availability and clustering
- Virtualisation
- Service hardening

Blended solutions are usually both economical and effective

Perimeter relay servers

Relay Servers

Provide I/O isolation and extend the features of your GWIAs

- Unsolicited bulk email filtering
- Anti-virus services
- Advanced SMTP connection management
- Enhanced logging
- Policy based message management
- Message retention features
- Auditing and analysis tools

Ideally provide fail over, clustering and load balancing features

Load Balancing

Software load balancing

- DNS round robin
- Perimeter relay servers
- GroupWise MTA routing
- Manual configurations

Hardware load balancing

- Can use service aware intelligence
- Can be used to implement ACLs
- Can be used to implement SSL offloading

Reverse proxies

- Can provide a blend of load balancing features

Hardware Load Balancing

Software Load Balancing

Performance

Using GroupWise components

Demarcations



User domains

User post offices



Service domains

Gateways

Identity Manager

Service post offices



Service post offices

System, service and application accounts

Mobile messaging connectivity

Access Control Lists (ACLs)

Demarcations

Prevent unauthorised access to services

Can be used to dedicate and optimise resources

Can be used to manage thin client access to services

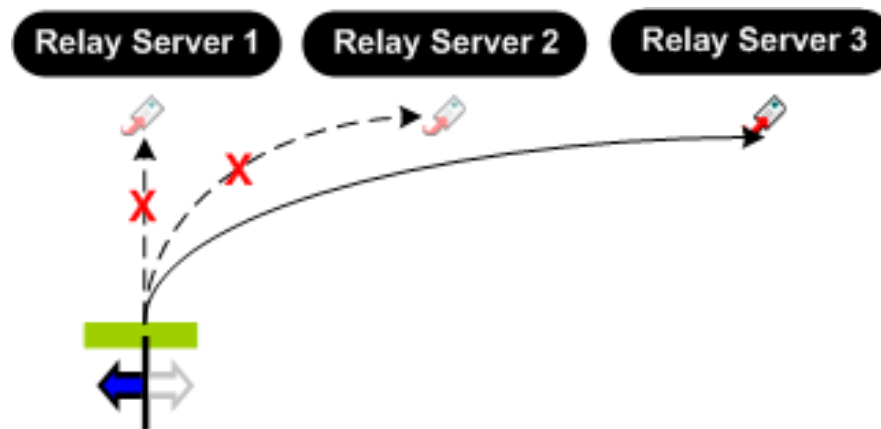
Can be implemented at many layers

Server firewalls can be used as ACL components

GroupWise Internet Agent Features

Redirection and Failover

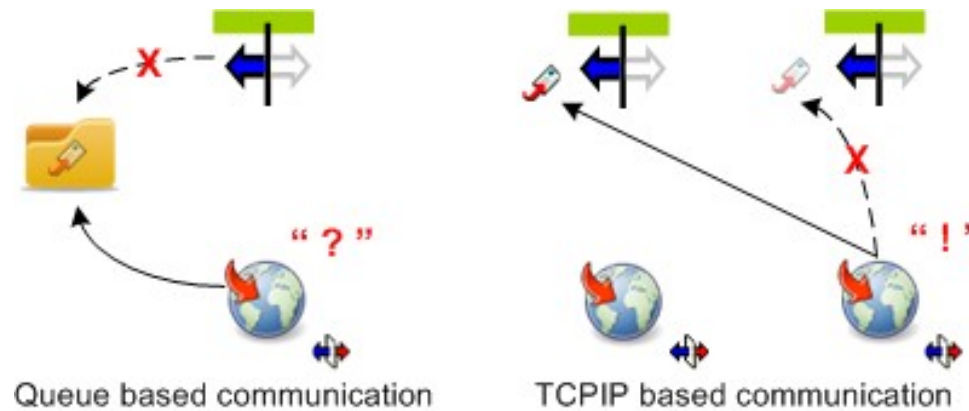
Multiple relay hosts for outbound messages



GroupWise Internet Agent Features

Redirection and Failover

Alternate Internet Agents



Clustering and virtualization

Service instances versus server and OS instances

Clustering

Virtualization

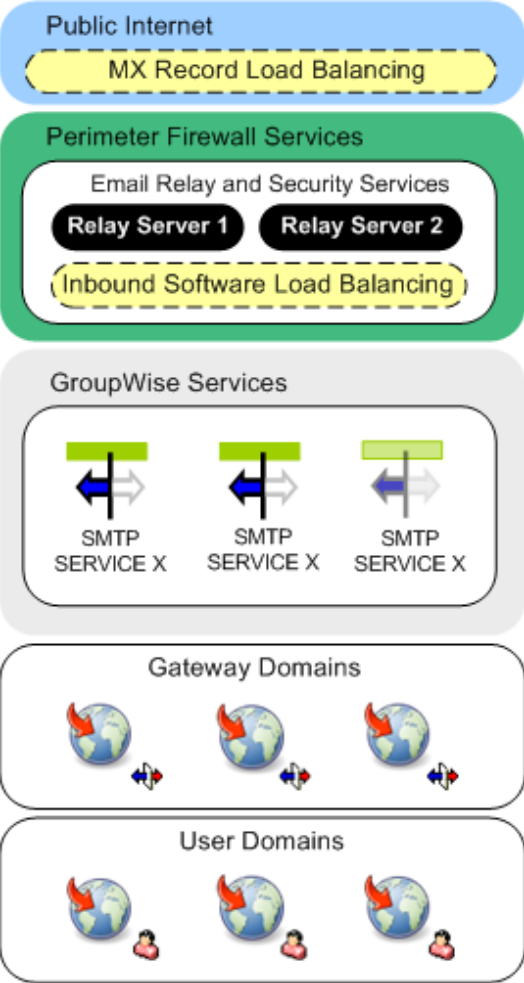
Novell®



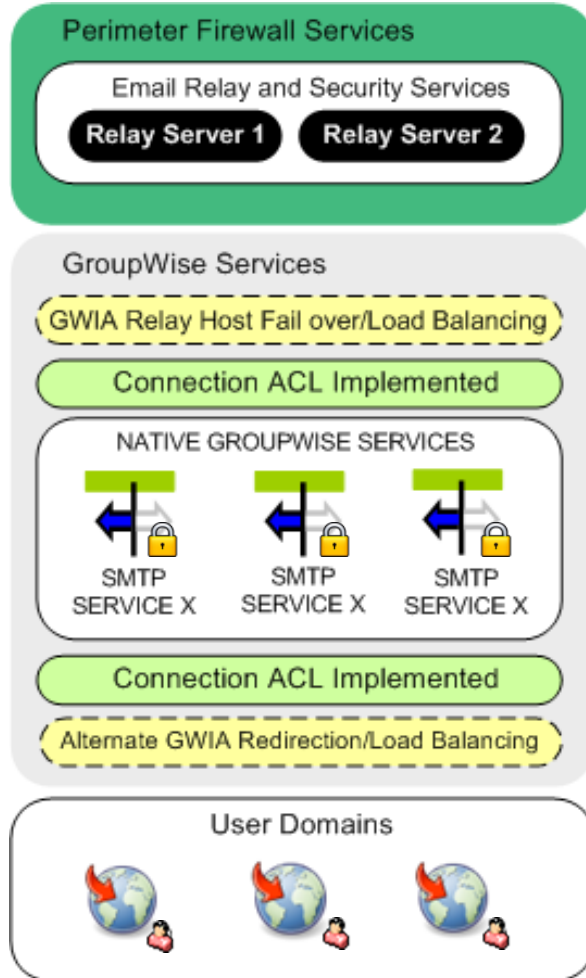
vmware®



Services for GroupWise clients



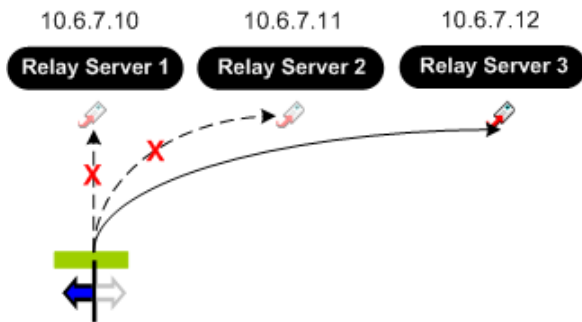
- Relay Servers
- Security
- Software Load Balancing
- Clustering
- Virtualization
- Performance



- Demarcations
- Connection ACL
- Redirection and Failover
- Software Load Balancing
- Performance

Multiple outbound relay hosts

Redirection and Failover



SMTP/MIME Settings

LDAP POP3/IMAP4 Server Directories Access Control Reattach Post Office Links GroupWise

Enable SMTP service

Number of SMTP send threads: 30

Number of SMTP receive threads: 75

Kill threads on exit or restart

Enable iCal service

Hostname/DNS "A Record" name: gwia2.yourdomain.edu

Relay Host for outbound messages: 10.6.7.10 10.6.7.11 10.6.7.12

Scan cycle for send directory: 10 seconds

Use 7 bit encoding for all outbound messages

Maximum number of hours to retry a deferred message: 96 hours

Intervals to retry a deferred message: 20,20,20,60

Return notification to sender when a message is delayed

Do not publish GroupWise information on an initial SMTP connection

Page Options... OK Cancel Apply Help

Alternate Internet Agents: GWIA MTP Settings

Redirection and Failover

LDAP | POP3/IMAP4 | Server Directories | Access Control | Reattach | Post Office Links | **GroupWise** | NDS

Network Address

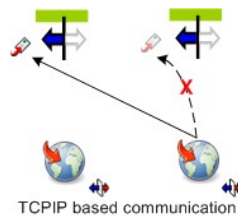
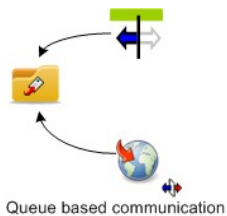
TCP/IP Address: gwia2.yourdomain.edu

IPX/SPX Address:

Bind Exclusively to TCP/IP Address

	Port	SSL	SSL Port
Message Transfer:	7102	Disabled	
HTTP:	9850	Required	
SMTP:	25	Disabled	
POP:	110	Disabled	995
IMAP:	143	Disabled	993
LDAP:	389	Disabled	636

Page Options... OK Cancel Apply Help



Alternate Internet Agents: User Domain Settings

Redirection and Failover



GroupWise NDS Rights Other Rights to Files and Folders

Internet Addressing

Override

Preferred Address format:
UserID@Internet domain name
Defined at: DVC_MAIL

Allowed Address Formats

UserID.Post Office@Internet domain name
 UserID@Internet domain name
 Last Name.First Name@Internet domain name
 First Name.Last Name@Internet domain name
 First Initial Last Name@Internet domain name
Defined at: DVC_MAIL

Internet domain name:
 yourdomain.edu
Defined at: DVC_MAIL
 For incoming mail, recipients are known exclusively by this Internet domain name

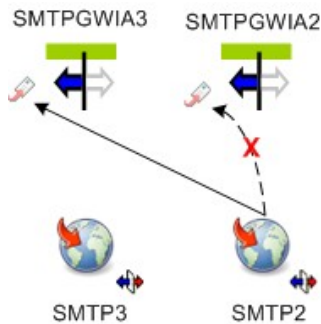
Internet Agent for outbound SMTP/MIME messages:
SMTP2.SMTPGWIA2
Defined at: DVC_MAIL

Alternate Internet Agent for outbound SMTP/MIME messages:
<None>

Page Options... OK Cancel Apply Help

Alternate Internet Agents: Gateway Domain Settings

Redirection and Failover



GroupWise Internet Addressing

Override Preferred Address format: UserID@Internet domain name
Defined at: DVC_MAIL

Allowed Address Formats
 UserID.Post Office@Internet domain name
 UserID@Internet domain name
 Last Name.First Name@Internet domain name
 First Name.Last Name@Internet domain name
 First Initial Last Name@Internet domain name
Defined at: DVC_MAIL

Internet domain name: yourdomain.edu
Defined at: DVC_MAIL
 For incoming mail, recipients are known exclusively by this Internet domain name

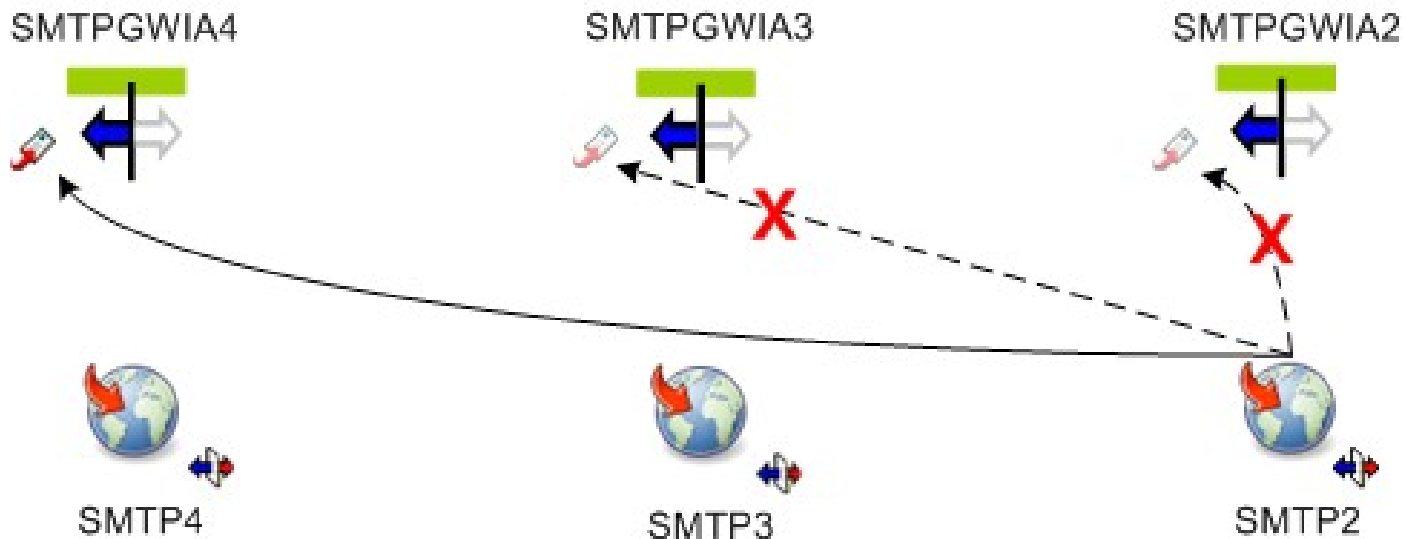
Internet Agent for outbound SMTP/MIME messages: SMTP2.SMTPGWIA2
Defined at: DVC_MAIL

Alternate Internet Agent for outbound SMTP/MIME messages: SMTP3.SMTPGWIA3

Page Options... OK Cancel Apply Help

Alternate Internet Agents: Gateway Chaining

Redirection and Failover



Internet Agent for outbound SMTP/MIME messages:

Defined at: DVC_MAIL

Alternate Internet Agent for outbound SMTP/MIME messages:

Internet Agent for outbound SMTP/MIME messages:

Defined at: DVC_MAIL

Alternate Internet Agent for outbound SMTP/MIME messages:

Internet Agent for outbound SMTP/MIME messages:

Defined at: DVC_MAIL

Alternate Internet Agent for outbound SMTP/MIME messages:

GWIA Access Control

Connection ACL

SMTP Connection ACL's

Implementing “Restricted” Internet Agents

Use to limit **inbound** access to protocols and connections

Required exceptions:

- Network addresses
- *@*.*
- Blank-Sender-User-ID

GWIA Access Control: Configuration

Connection ACL

The screenshot shows the 'SMTP Incoming' configuration window. The 'SMTP Incoming Defaults' section has three radio buttons: 'Inherit access' (unselected), 'Allow incoming messages' (unselected), and 'Prevent incoming messages' (selected). Below this, there is a checked checkbox 'Prevent messages larger than' followed by a spinner box containing '27648' and the text 'Kbytes'. The 'Exceptions' section is highlighted with a red border and contains two list boxes. The 'Allow messages from:' list box contains the following entries: '*@*', 'Blank-Sender-User-ID', 'relayserver1.domain.edu', 'relayserver2.domain.edu', 'relayserver3.domain.edu', '10.6.7.10', '10.6.7.11', and '10.6.7.12'. The 'Prevent messages from:' list box is currently empty. Both list boxes have 'Create...', 'Edit...', and 'Delete' buttons below them. On the right side of the dialog, there are 'OK', 'Cancel', and 'Help' buttons.

GWIA Access Control: Configuration

Relay ACL

The screenshot shows the 'Access Control' configuration window for 'SMTP Relay Settings'. The window has a menu bar with 'SMTP/MIME', 'LDAP', 'POP3/IMAP4', 'Server Directories', 'Access Control', 'Reattach', 'Post Office Links', and 'Group'. The 'Access Control' menu is open, showing 'SMTP Relay Settings'. The main area is divided into 'SMTP Relay Defaults' and 'Exceptions'. In 'SMTP Relay Defaults', there are two radio buttons: 'Allow message relaying' (unselected) and 'Prevent message relaying' (selected). Below this is a checkbox 'Prevent messages larger than' followed by a text box and 'Kbytes'. The 'Exceptions' section has two tables: 'Allow:' and 'Prevent:'. Each table has columns for 'From' and 'To'. To the right of each table are buttons for 'Create...', 'Edit...', and 'Delete'. At the bottom of the window are buttons for 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help'.

SMTP/MIME | LDAP | POP3/IMAP4 | Server Directories | **Access Control** | Reattach | Post Office Links | Group

SMTP Relay Settings

SMTP Relay Defaults

Allow message relaying

Prevent message relaying

Prevent messages larger than Kbytes

Exceptions

Allow:

From	To
------	----

Create...
Edit...
Delete

Prevent:

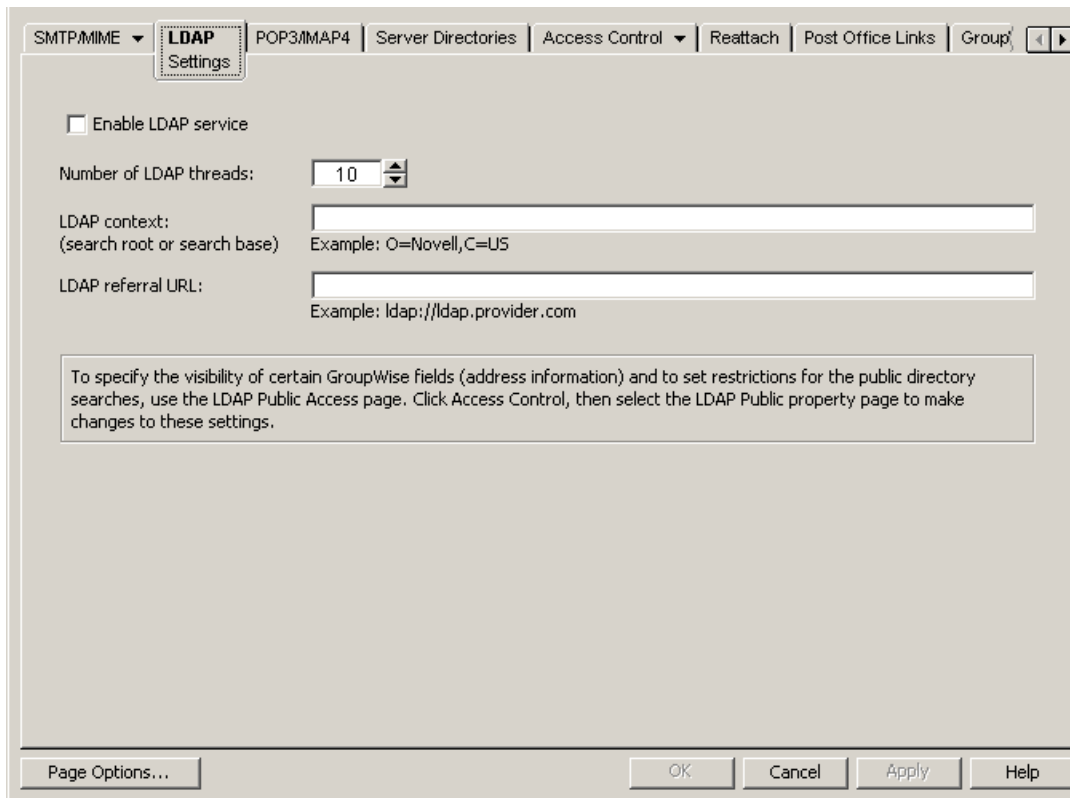
From	To
------	----

Create...
Edit...
Delete

Page Options... | OK | Cancel | Apply | Help

GWIA Access Control: Configuration

Connection ACL



The screenshot shows the 'LDAP Settings' window within the GroupWise configuration interface. The window title bar includes tabs for 'SMTP/MIME', 'LDAP Settings', 'POP3/IMAP4', 'Server Directories', 'Access Control', 'Reattach', 'Post Office Links', and 'Group'. The 'LDAP Settings' tab is active. The configuration options are as follows:

- Enable LDAP service
- Number of LDAP threads: 10 (spin box)
- LDAP context: (search root or search base) Example: O=Novell,C=US
- LDAP referral URL: Example: ldap://ldap.provider.com

A text box at the bottom of the window contains the following instruction:

To specify the visibility of certain GroupWise fields (address information) and to set restrictions for the public directory searches, use the LDAP Public Access page. Click Access Control, then select the LDAP Public property page to make changes to these settings.

At the bottom of the window, there are buttons for 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help'.

GWIA Access Control: Configuration

Connection ACL

The screenshot displays the 'POP3/IMAP4 Settings' window in the GroupWise Administration Console. The window has a tabbed interface with the following tabs: SMTP/MIME, LDAP, POP3/IMAP4 Settings (selected), Server Directories, Access Control, Reattach, Post Office Links, and GroupWise. The 'POP3' section contains the following settings:

- Enable POP3 service
- Number of threads for POP3 connections: 30
- Number of threads for POP3 SSL connections: 30
- Enable intruder detection
- Do not publish GroupWise information on an initial POP3 connection

The 'IMAP4' section contains the following settings:

- Enable IMAP4 service
- Number of threads for IMAP4 connections: 30
- Number of threads for IMAP4 SSL connections: 30
- Maximum number of items to read (in thousands): 0
- Do not publish GroupWise information on an initial IMAP4 connection

At the bottom of the window, there are buttons for 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help'.

GWIA Configuration: Configuration

Performance

The screenshot shows the 'Performance' tab of the 'SMTP/MIME Timeouts' configuration window. The window has a title bar with 'SMTP/MIME' and 'Timeouts'. Below the title bar are several tabs: 'LDAP', 'POP3/IMAP4', 'Server Directories', 'Access Control', 'Reattach', 'Post Office Links', and 'Group'. The 'SMTP/MIME' tab is selected. The main area contains six settings, each with a numeric input field and a 'minutes' label:

Setting	Value	Unit
Commands:	5	minutes
Data:	3	minutes
Connection Establishment:	1	minutes
Initial Greeting:	5	minutes
TCP Read:	5	minutes
Connection Termination:	5	minutes

At the bottom of the window are four buttons: 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help'.

System benchmark results

Performance

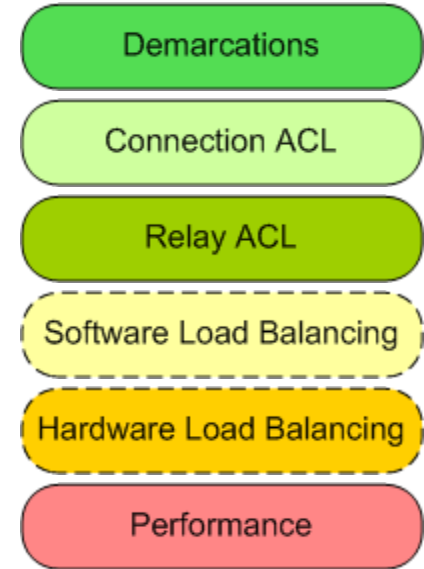
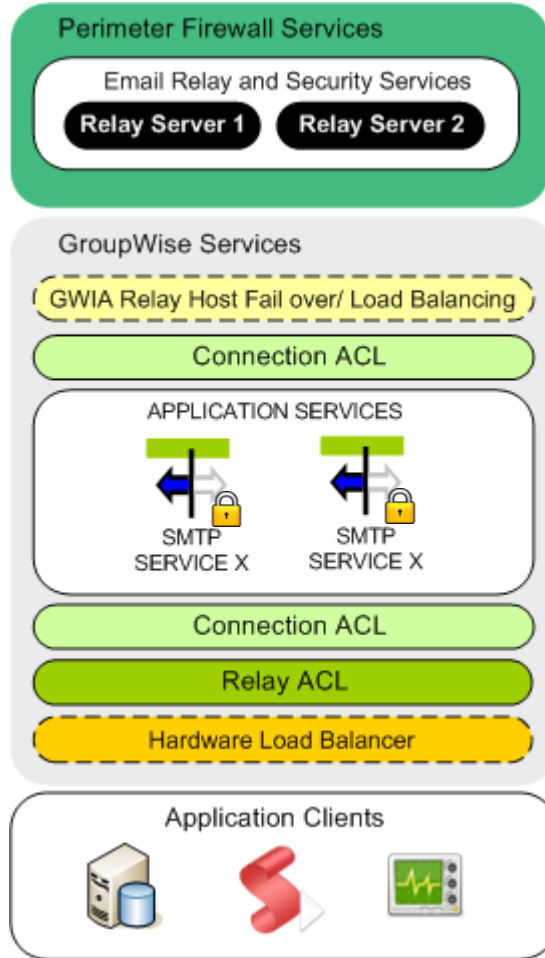
90 – 95% reduction in unwanted email at the perimeter

Quantifiable delivery performance increases

Unscheduled service downtime eliminated

Attachment sizes could be increased without performance penalties

Services for Application clients



Security

Unmanaged client examples

Thin clients (applications, SQL and PowerShell scripts)

Desktop and mobile POP and IMAP clients

Other services “consuming” GroupWise services

Blackberry Internet Service (BIS)

Gmail

Notify Link



Additional security concerns

Security

Data leakage and loss

Anti-virus and malware infections

Cannot secure or audit third party “local” message stores

Cannot remotely manage or wipe unauthorized devices

GWIA Access Control: Configuration

Connection ACL

The screenshot shows the 'SMTP Incoming' configuration window. It has tabs for 'SMTP Incoming', 'SMTP Outgoing', 'IMAP4', and 'POP3'. The 'SMTP Incoming Defaults' section contains three radio buttons: 'Inherit access', 'Allow incoming messages', and 'Prevent incoming messages', with the last one selected. Below this is a checked checkbox 'Prevent messages larger than' followed by a spinner box set to '10978' and the text 'Kbytes'. The 'Exceptions' section has two list boxes: 'Allow messages from:' and 'Prevent messages from:'. The 'Allow messages from:' list contains: '*@.*', 'Blank-Sender-User-ID', 'relayserver1.domain.edu', 'relayserver2.domain.edu', '10.6.7.13', '10.6.7.14', '10.7.8.45', '10.7.9.110', and '10.7.10.122'. Below the list boxes are 'Create...', 'Edit...', and 'Delete' buttons for each. On the right side of the dialog are 'OK', 'Cancel', and 'Help' buttons.

GWIA Access Control: Configuration

Relay ACL

The screenshot shows the 'Access Control' configuration window for SMTP Relay Settings. The 'SMTP Relay Defaults' section has two radio buttons: 'Allow message relaying' (unselected) and 'Prevent message relaying' (selected). Below this, there is a checked checkbox for 'Prevent messages larger than' with a value of '10978' Kbytes. The 'Exceptions' section contains two tables: 'Allow' and 'Prevent'. The 'Allow' table lists IP addresses in the 'From' column and domains in the 'To' column. The 'Prevent' table is currently empty.

From	To
10.7.8.12	*
10.8.12.45	*
10.8.12.100	someotherdomain.com
10.9.2.23	*
10.9.3.33	newfound.edu
10.9.3.50	*

From	To
------	----

GWIA Access Control: Configuration

Connection ACL

SMTP/MIME | LDAP | POP3/IMAP4 | Server Directories | **Access Control** | Reattach | Post Office Links | Group

Settings

Class of Service:

Default Class of Service
Application POP-IMAP Access

Create...
Edit...
Delete

Memberships:

Member ID	Post Office	Domain
APPLICATION_POP_IMAP	VXPO1	VXDOMAIN1

Add...
Remove

Test

Page Options... | OK | Cancel | Apply | Help

GWIA Access Control: Configuration

Connection ACL

SMTP Incoming | SMTP Outgoing | IMAP4 | POP3

SMTP Incoming Defaults

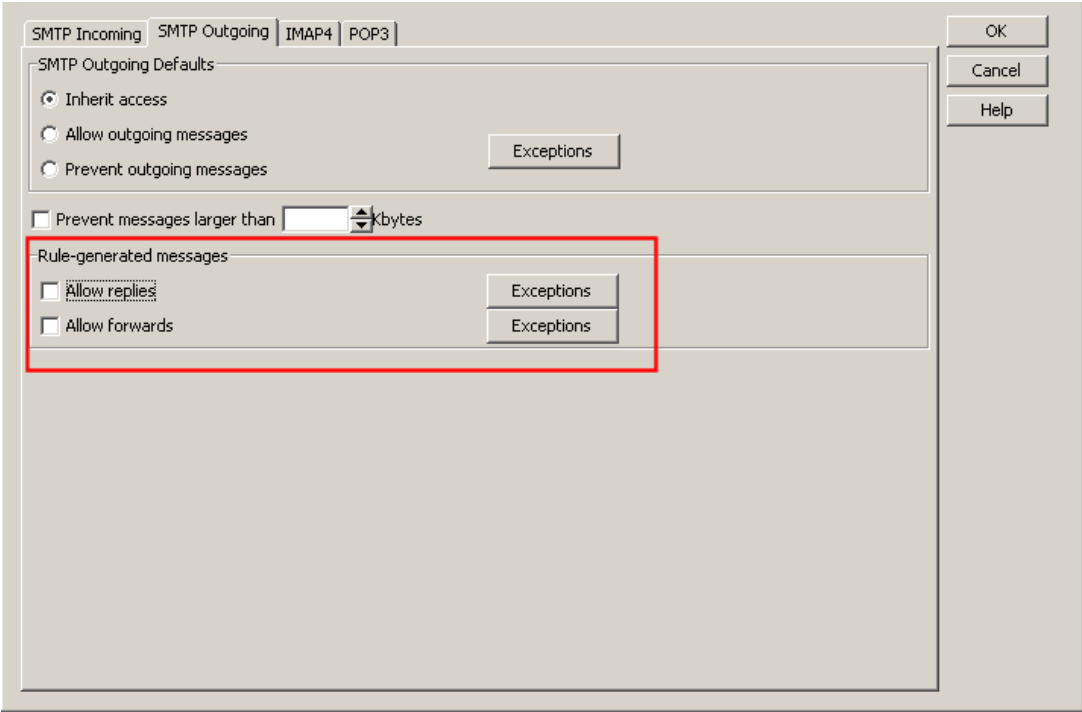
- inherit access
- Allow incoming messages
- Prevent incoming messages

Access will be decided based on the settings in the Default Class of Service or through membership in another Class of Service.

OK
Cancel
Help

GWIA Access Control: Configuration

Connection ACL



The screenshot shows a configuration dialog box for GWIA Access Control. It has four tabs: SMTP Incoming, SMTP Outgoing, IMAP4, and POP3. The SMTP Outgoing tab is selected. The dialog is divided into two main sections: SMTP Outgoing Defaults and Rule-generated messages. In the SMTP Outgoing Defaults section, there are three radio buttons: 'Inherit access' (selected), 'Allow outgoing messages', and 'Prevent outgoing messages'. An 'Exceptions' button is located to the right of these options. Below this is a checkbox for 'Prevent messages larger than' followed by a text input field and a 'Kbytes' label. In the Rule-generated messages section, there are two checkboxes: 'Allow replies' and 'Allow forwards'. Each checkbox has an 'Exceptions' button to its right. A red rectangular box highlights the 'Allow replies' and 'Allow forwards' options and their respective 'Exceptions' buttons. On the right side of the dialog, there are three buttons: 'OK', 'Cancel', and 'Help'.

GWIA Access Control: Configuration

Connection ACL

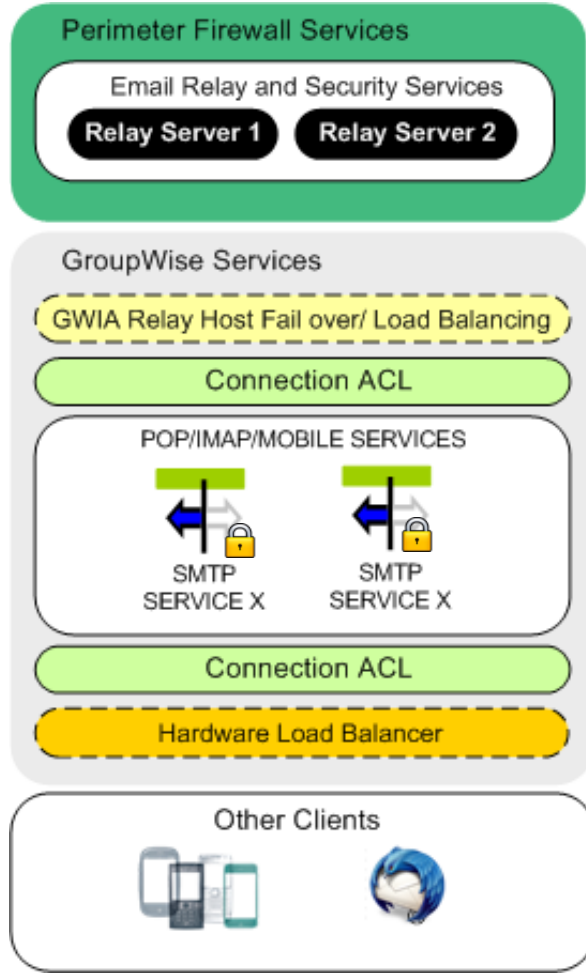
The screenshot shows a configuration dialog box with tabs for SMTP Incoming, SMTP Outgoing, IMAP4, and POP3. The IMAP4 tab is selected. Inside the dialog, there is a section titled "IMAP4 Defaults" containing three radio button options: "inherit access", "Allow access", and "Prevent access". The "Allow access" option is currently selected. To the right of the dialog are three buttons: "OK", "Cancel", and "Help".

GWIA Access Control: Configuration

Connection ACL

The screenshot shows a configuration dialog box for GWIA Access Control, specifically the POP3 Defaults tab. The dialog has a title bar with tabs for SMTP Incoming, SMTP Outgoing, IMAP4, and POP3. The POP3 Defaults section contains three radio buttons: 'inherit access' (selected), 'Allow access', and 'Prevent access'. Below this are four checkboxes: 'Delete messages from GroupWise mailbox after download' (unchecked), 'Purge messages from GroupWise mailbox after download' (unchecked), 'Convert messages to MIME format when downloading' (checked), and 'High performance on file size calculations' (unchecked). At the bottom, there are two spinners: 'Number of Days Prior to Today to Get Messages From:' set to 30, and 'Maximum Number of Messages to Download:' set to 100. On the right side of the dialog, there are three buttons: OK, Cancel, and Help.

Services for POP and IMAP clients



- Demarcations
- Connection ACL
- Software Load Balancing
- Hardware Load Balancing
- Performance

GWIA Access Control: Configuration

Connection ACL

SMTP/MIME | LDAP | **POP3/IMAP4 Settings** | Server Directories | Access Control | Reattach | Post Office Links | GroupWise

POP3

- Enable POP3 service
- Number of threads for POP3 connections: 30
- Number of threads for POP3 SSL connections: 30
- Enable intruder detection
- Do not publish GroupWise information on an initial POP3 connection

IMAP4

- Enable IMAP4 service
- Number of threads for IMAP4 connections: 30
- Number of threads for IMAP4 SSL connections: 30
- Maximum number of items to read (in thousands): 0
- Do not publish GroupWise information on an initial IMAP4 connection

Page Options... | OK | Cancel | Apply | Help

GWIA Access Control: Configuration

Connection ACL

The screenshot shows the 'SMTP Incoming' configuration window. At the top, there are tabs for 'SMTP Incoming', 'SMTP Outgoing', 'IMAP4', and 'POP3'. The 'SMTP Incoming Defaults' section contains three radio buttons: 'Inherit access', 'Allow incoming messages', and 'Prevent incoming messages', with the third option selected. Below this, a checkbox labeled 'Prevent messages larger than' is checked, with a value of '27648' in a text box and 'Kbytes' as the unit. The 'Exceptions' section has two list boxes: 'Allow messages from:' and 'Prevent messages from:'. The 'Allow messages from:' list contains the following entries: '*@.*', 'Blank-Sender-User-ID', 'loadbalancer1.domain.edu', 'loadbalancer2.domain.edu', 'relayserver1.domain.edu', 'relayserver2.domain.edu', '10.6.7.11', '10.6.7.12', and '10.6.7.13'. Below each list box are 'Create...', 'Edit...', and 'Delete' buttons. On the right side of the dialog, there are 'OK', 'Cancel', and 'Help' buttons.

GWIA Access Control: Configuration

Relay ACL

The screenshot shows the 'Access Control' configuration window for SMTP Relay Settings. The window has a menu bar with 'SMTP/MIME', 'LDAP', 'POP3/IMAP4', 'Server Directories', 'Access Control', 'Reattach', 'Post Office Links', and 'Group'. The 'Access Control' menu is open, showing 'SMTP Relay Settings' as the selected option. The main area is divided into several sections:

- SMTP Relay Defaults:** Contains two radio buttons: 'Allow message relaying' (unselected) and 'Prevent message relaying' (selected).
- Prevent messages larger than:** A checkbox is unchecked, followed by a text input field and a 'Kbytes' label.
- Exceptions:** Divided into 'Allow:' and 'Prevent:' sections. Each section has a table with 'From' and 'To' columns and a vertical scrollbar. To the right of each table are three buttons: 'Create...', 'Edit...', and 'Delete'.

At the bottom of the window, there are four buttons: 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help'.

GWIA Access Control: Notes

Relay ACL

Security



Technical Notes: /forceinboundauth and --forceinboundauth switches

Requires clients to authenticate before using SMTP services

GWIA relay configuration is null for clients that authenticate



Minimally SSL connections should be enforced to reduce risks

GWIA Access Control: Notes

Relay ACL

SMTP Relay ACL's

SMTP Relay "truth table"

Relay Exception: None

From	To	GWIA Relays	Relay Server Delivers
<Any known iDomain>	<Foreign Domain>	NO	N/A
<Foreign Domain>	<Any known iDomain>	YES	N/A
<Any known iDomain>	<Any known iDomain>	YES	N/A
<Foreign Domain>	<Foreign Domain>	NO	N/A

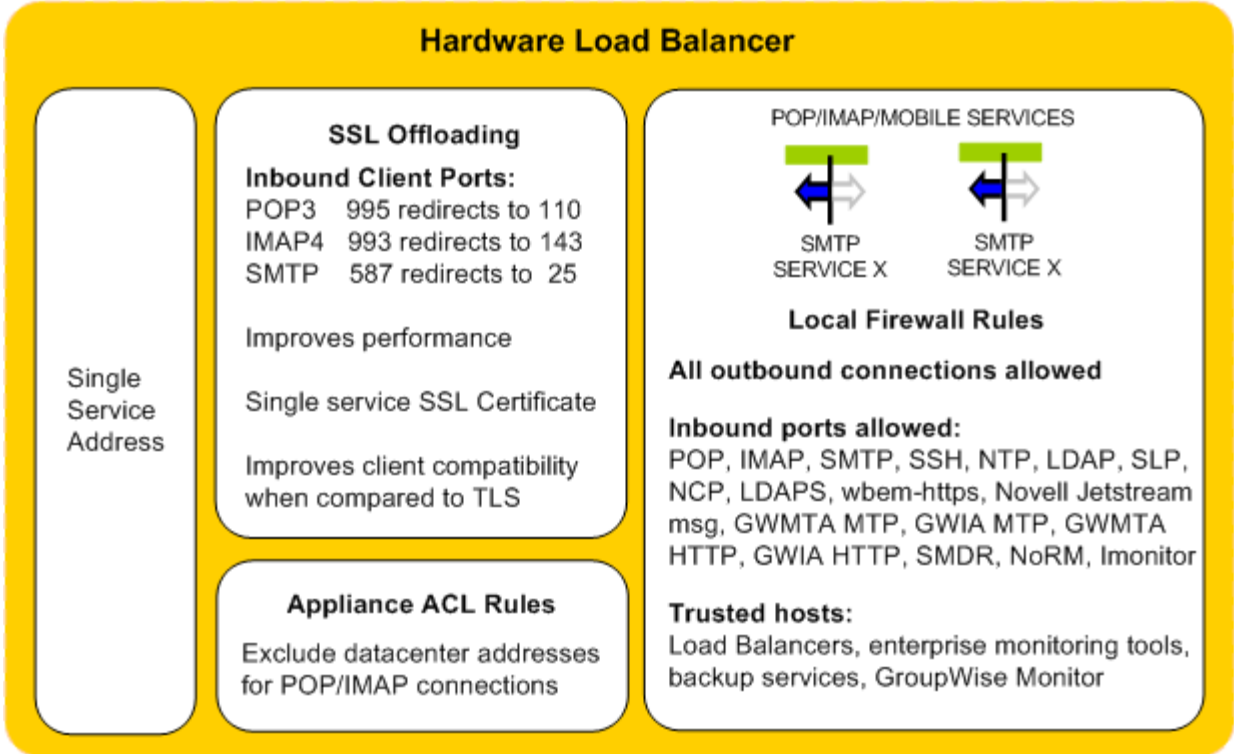
Relay Exception: someiDomain.com

From	To	GWIA Relays	Relay Server Delivers
<Any known iDomain>	<Foreign Domain>	NO	N/A
<Foreign Domain>	<Any known iDomain>	YES	N/A
<Any known iDomain>	<Any known iDomain>	YES	N/A
<Foreign Domain>	<Foreign Domain>	NO	N/A

Relay Exception: *

From	To	GWIA Relays	Relay Server Delivers
<Any known iDomain>	<Foreign Domain>	YES	YES
<Foreign Domain>	<Any known iDomain>	YES	N/A
<Any known iDomain>	<Any known iDomain>	YES	N/A
<Foreign Domain>	<Foreign Domain>	YES	NO

What should happen inside your load balancer ...



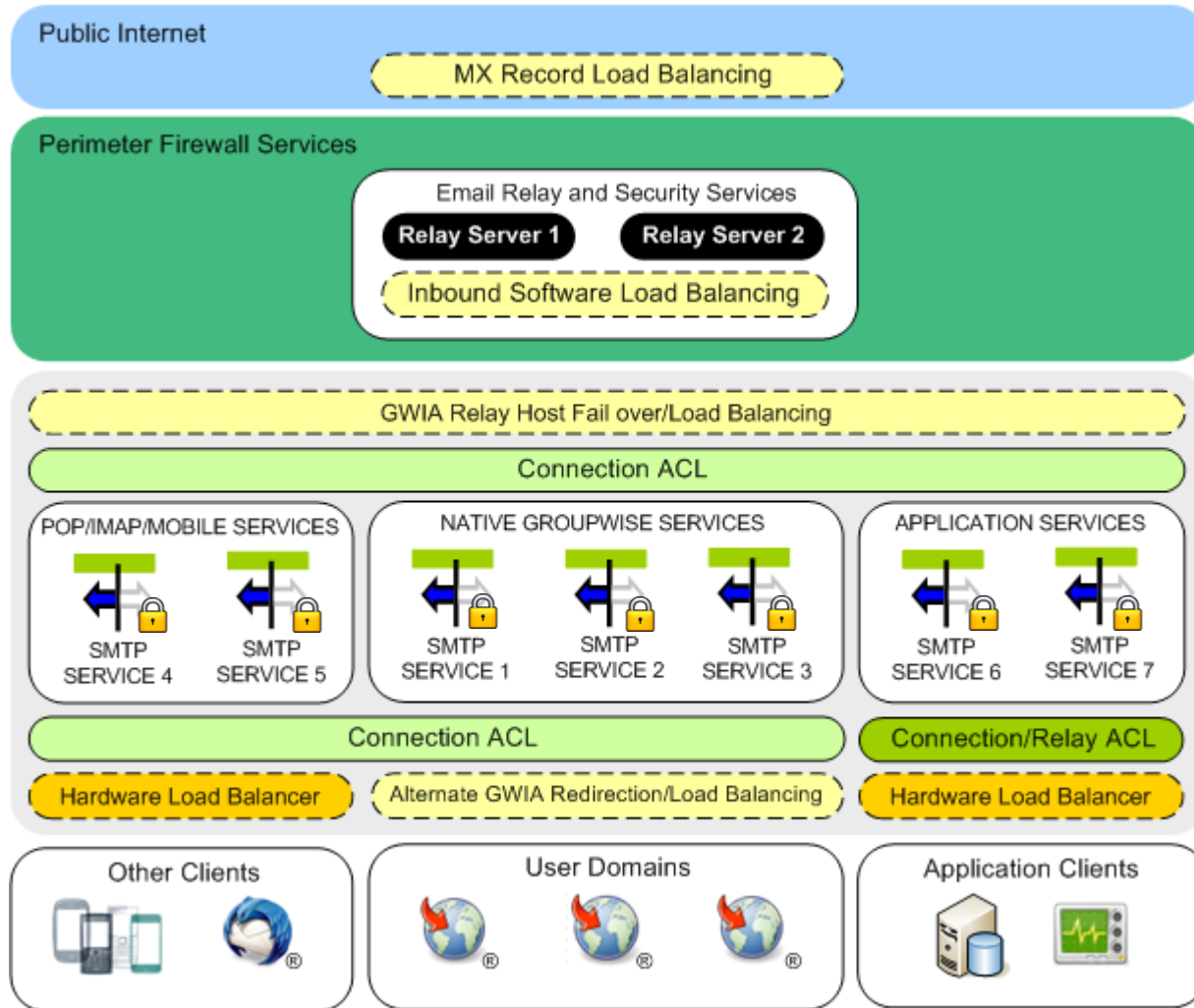
SuSE Linux server: Configuration

The /etc/SuSEconfig/SuSEfirewall2 configuration file:

```
FW_SERVICES_EXT_TCP="123 1500 1501 1578 1579 1581 22 389  
40193 427 524 5989 636 6901 7100 7102  
7180 8008 8009 8028 8030 9850"
```

```
FW_SERVICES_EXT_UDP="123 427 524"
```

```
FW_TRUSTED_NETS="10.6.7.13/32,tcp,110 10.6.7.13/32,tcp,143  
10.6.7.13/32,tcp,25 10.6.7.14/32,tcp,110  
10.6.7.14/32,tcp,143 10.6.7.14/32,tcp,25  
10.6.7.15/32,tcp,110 10.6.7.15/32,tcp,143  
10.6.7.15/32,tcp,25 10.6.7.10,tcp,8400"
```

Technical and configuration details

GroupWise Best Practices wiki

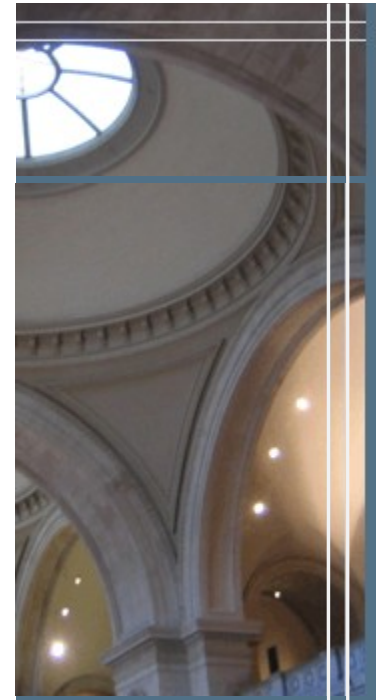


<http://wiki.novell.com/index.php/GroupWise>

Architecture and concept details:



http://www.lawrencekearney.com/files/OpenHorizons_Issue_15_SMTP_Onion.pdf



GroupWise SMTP Infrastructure Design

Thank you for your time and attendance !