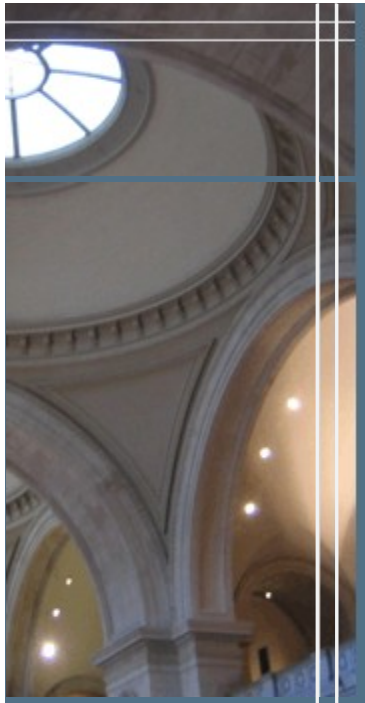


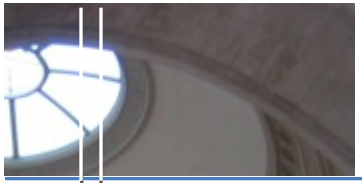
Technology Transfer Partners

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



Session Agenda

Focus on the technical aspects of design, deployment and configuration

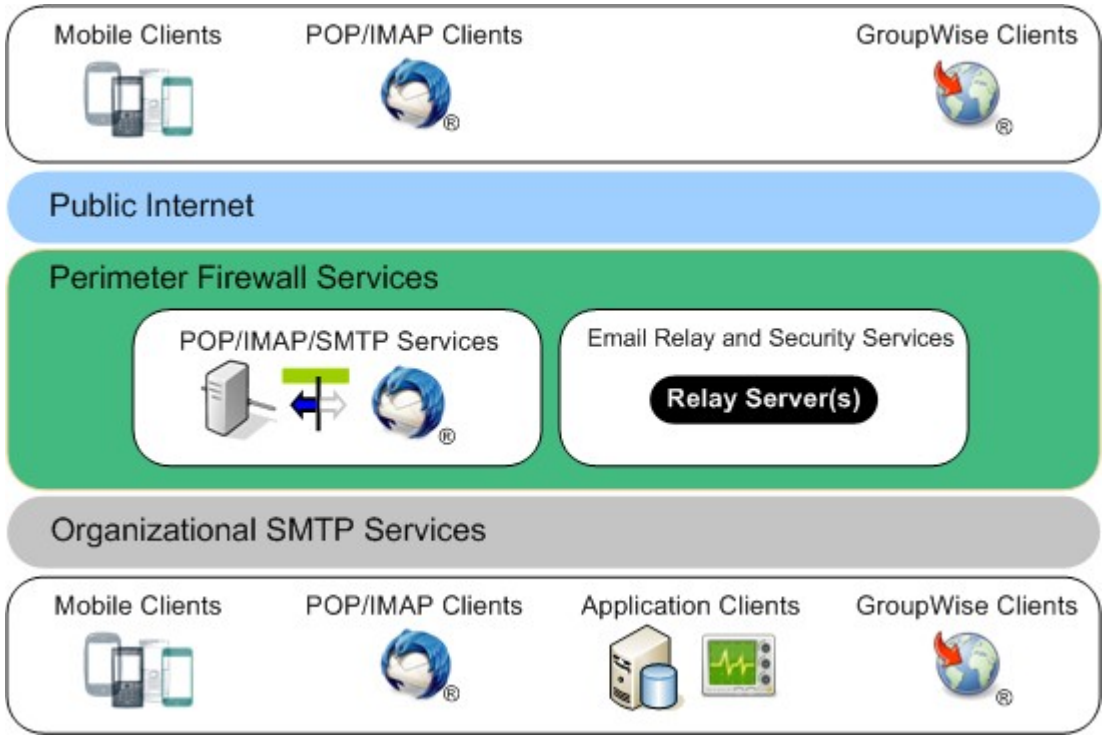
Most information applies to large and enterprise size environments

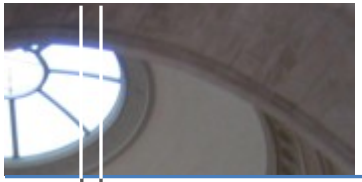
Designing systems to compete with similar commercial service offerings

Maximizing value using basic infrastructure resources

A typical enterprise environment

Services normally compete for system resources





How well a service does when measured ...

Performance

Stability

Features

Cost of ownership

Scaling

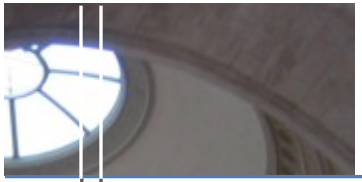
Security

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



What can we do to improve services?

- 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

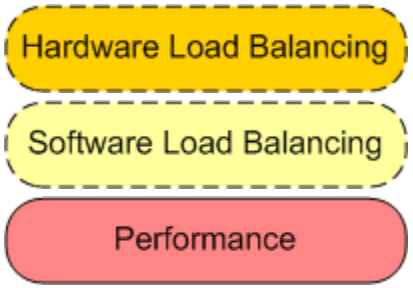
Perimeter relay servers

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

Using GroupWise components

Demarcations

User domains

User post offices

Service domains

Gateways

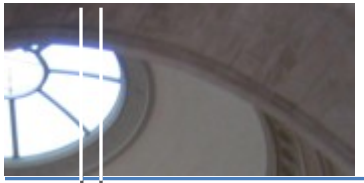
Identity Manager

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

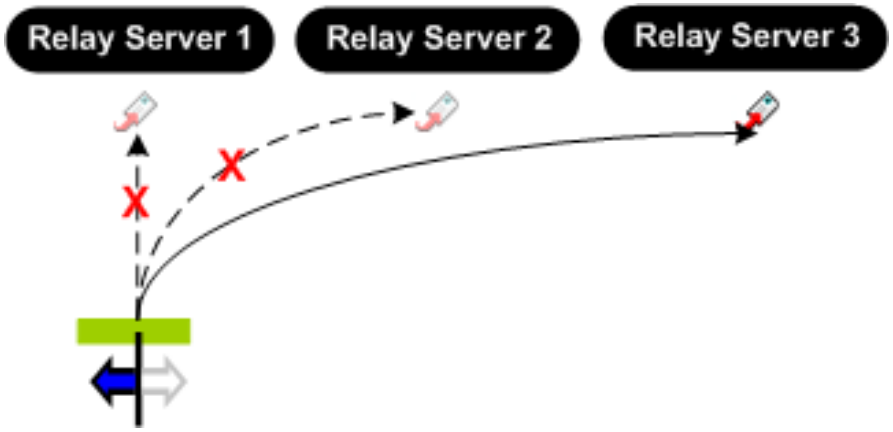
Can be implemented at many layers

Server firewalls can be used as ACL components

GroupWise Internet Agent Features

Redirection and Failover

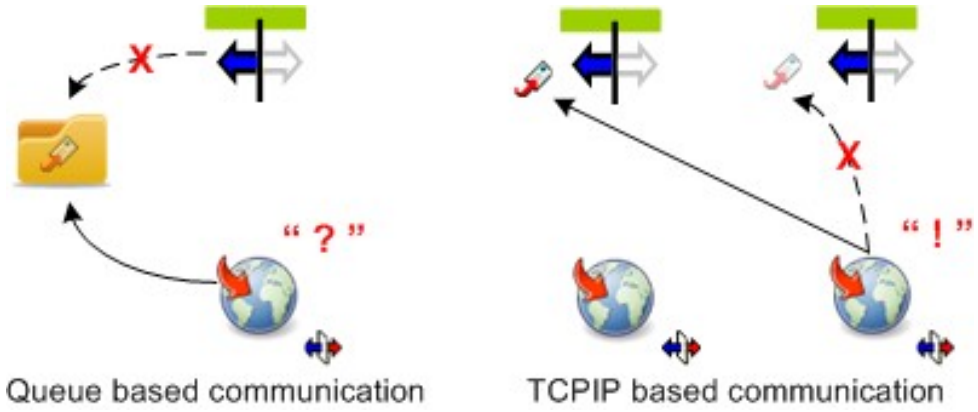
Multiple relay hosts for outbound messages



GroupWise Internet Agent Features

Redirection and Failover

Alternate Internet Agents



Clustering and virtualization

Service instances versus server and OS instances

Clustering

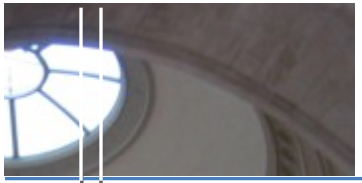
Virtualization

Novell

Microsoft

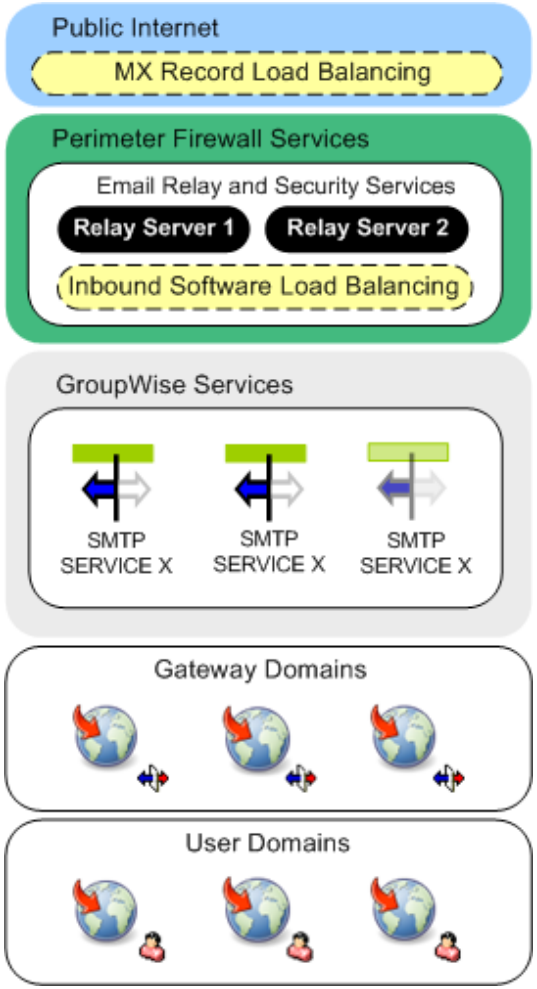
Xen™

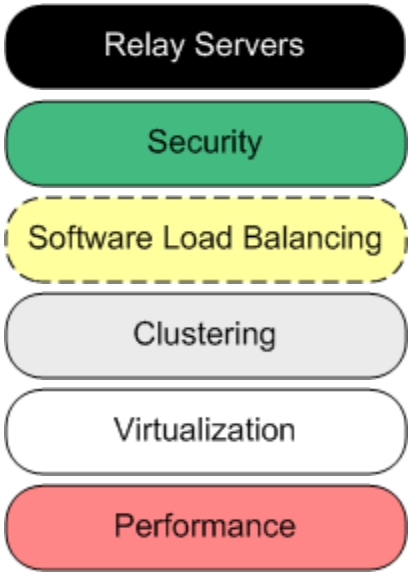
vmware®



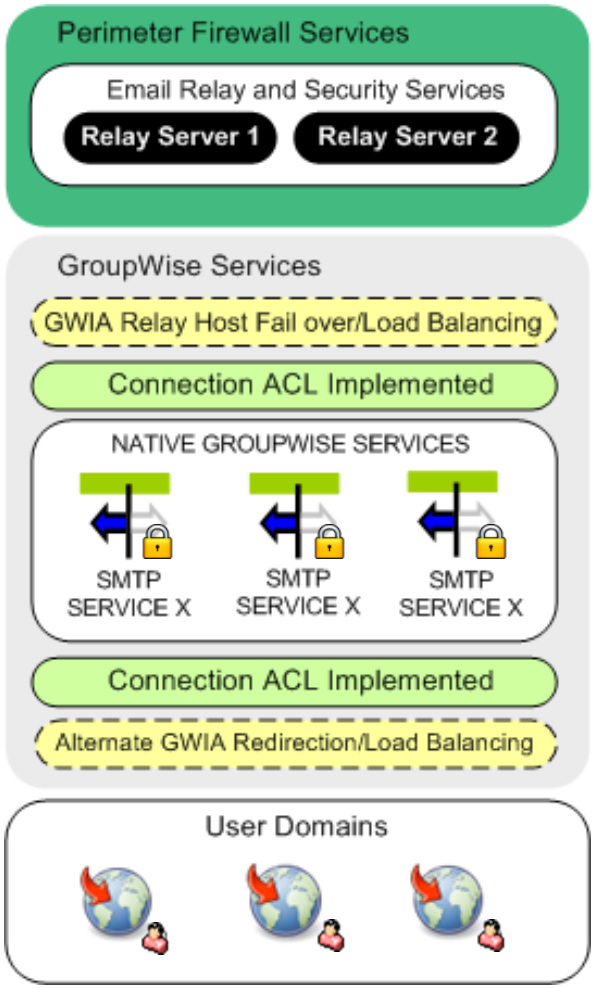
Services for GroupWise clients

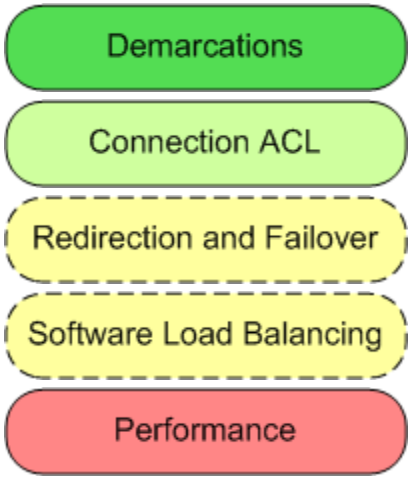
Load Balancing Inbound Mail





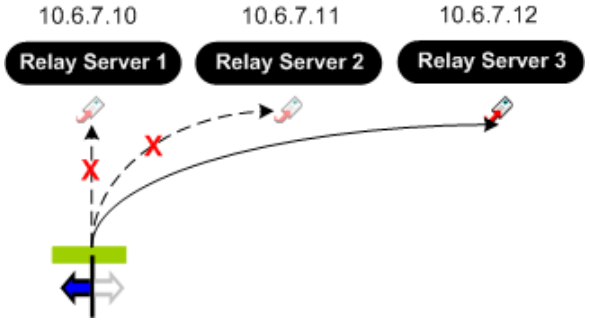
Load Balancing Outbound Mail

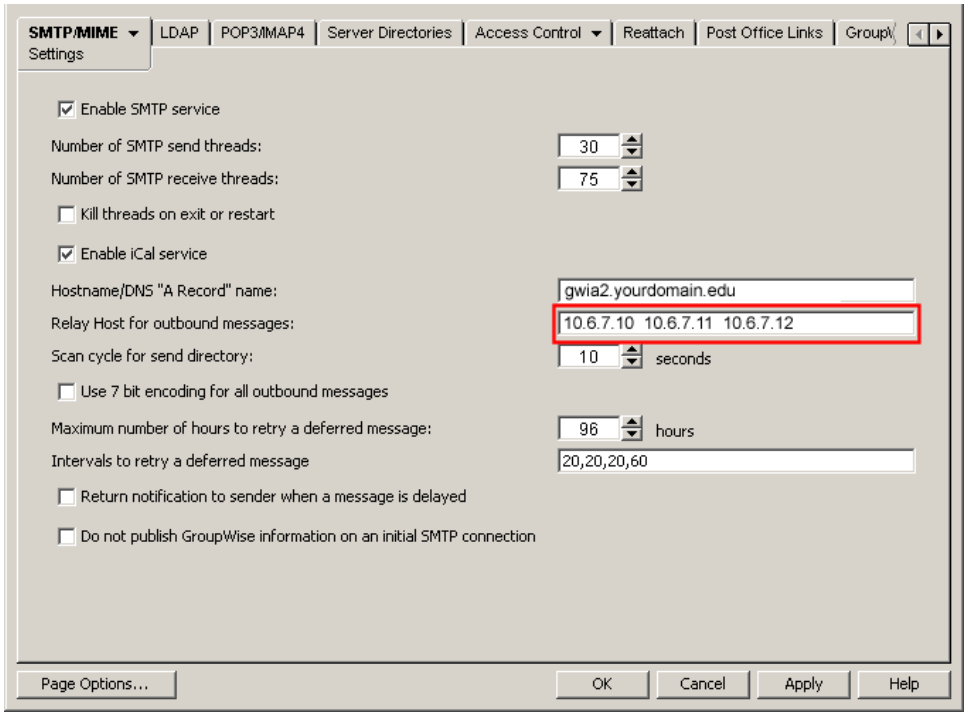




Multiple outbound relay hosts

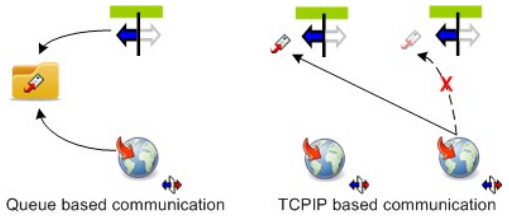
Redirection and Failover

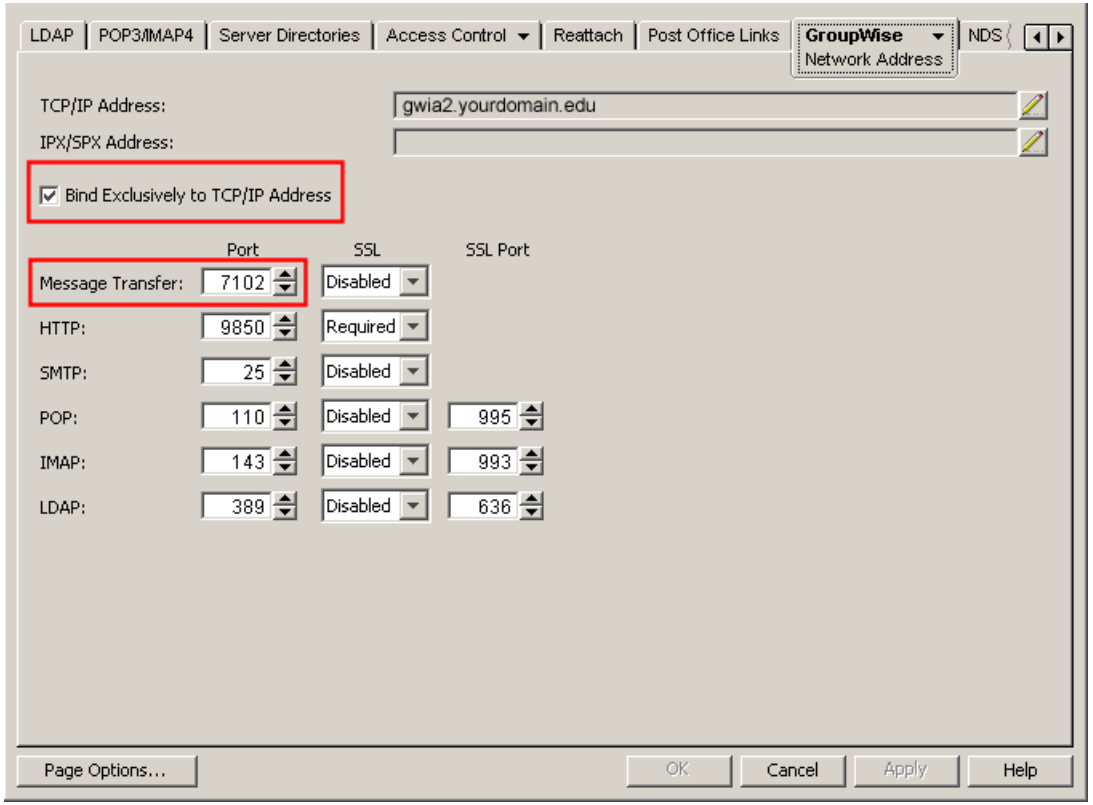




Alternate Internet Agents: GWIA MTP Settings

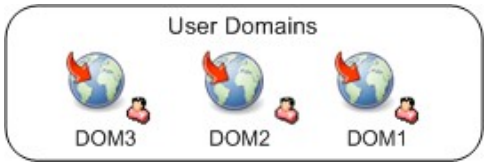
Redirection and Failover

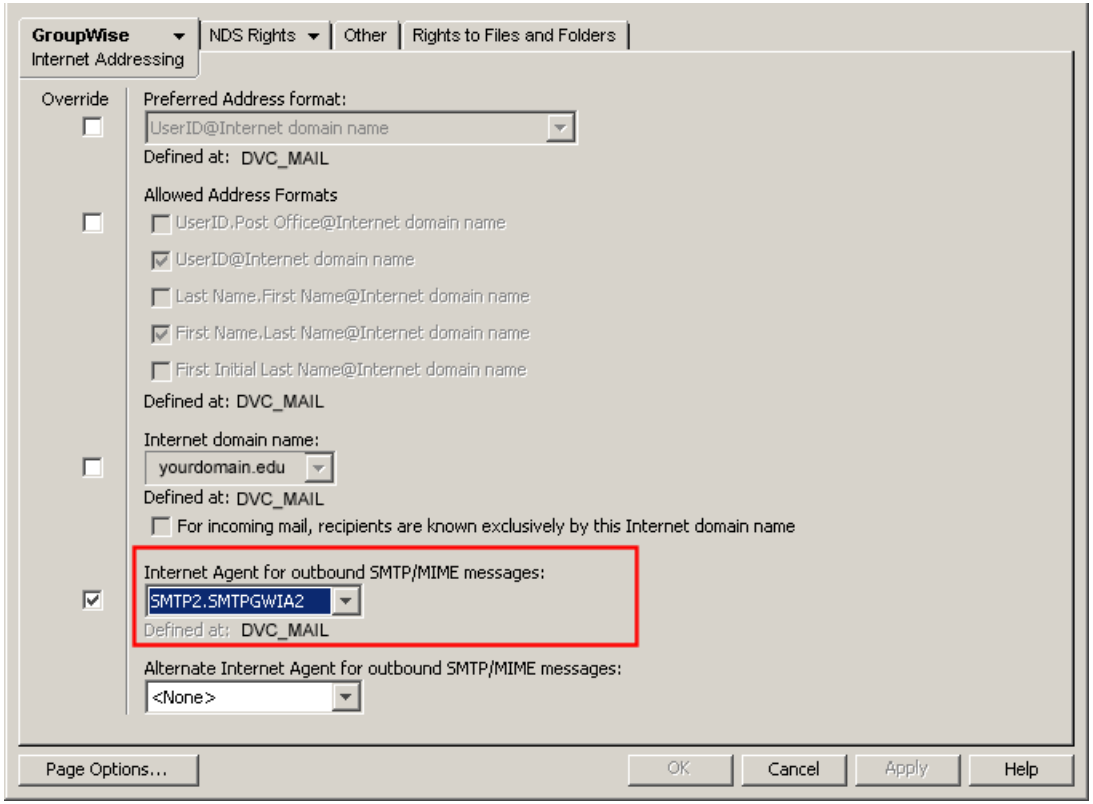




Alternate Internet Agents: User Domain Settings

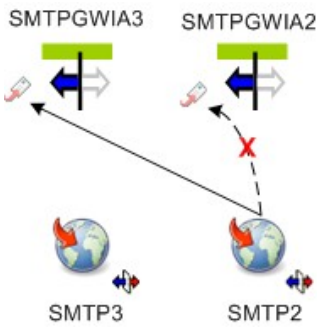
Redirection and Failover

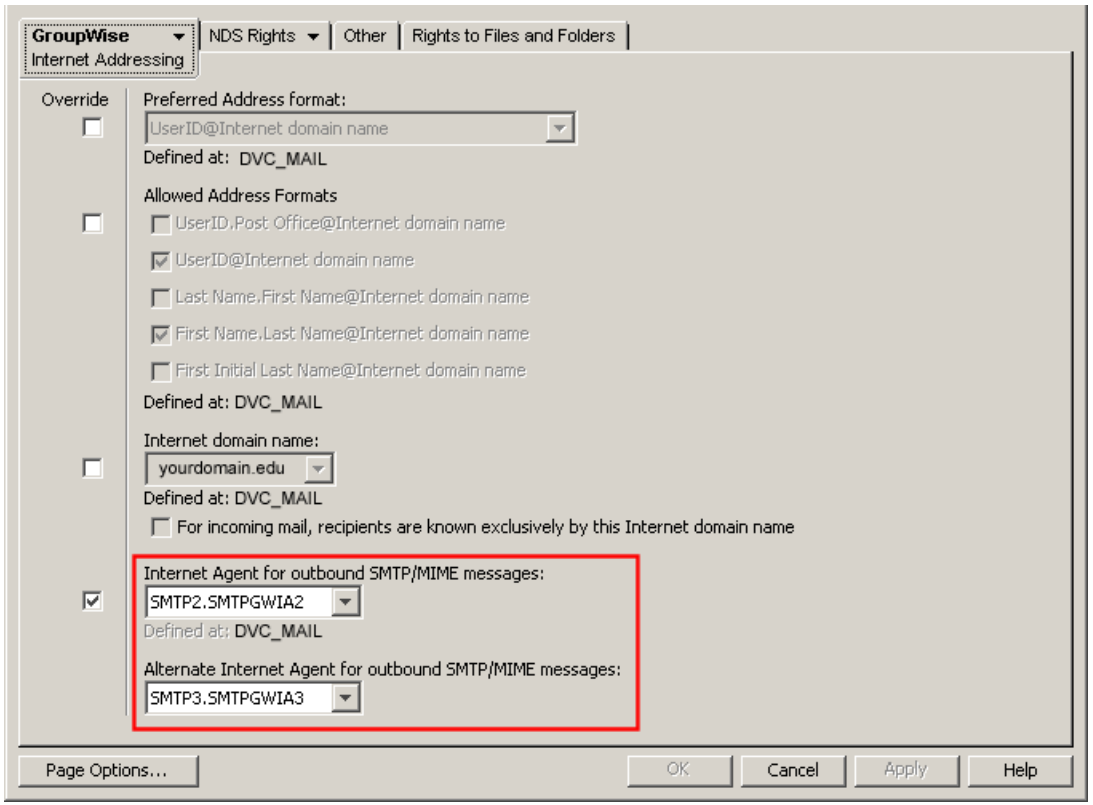




Alternate Internet Agents: Gateway Domain Settings

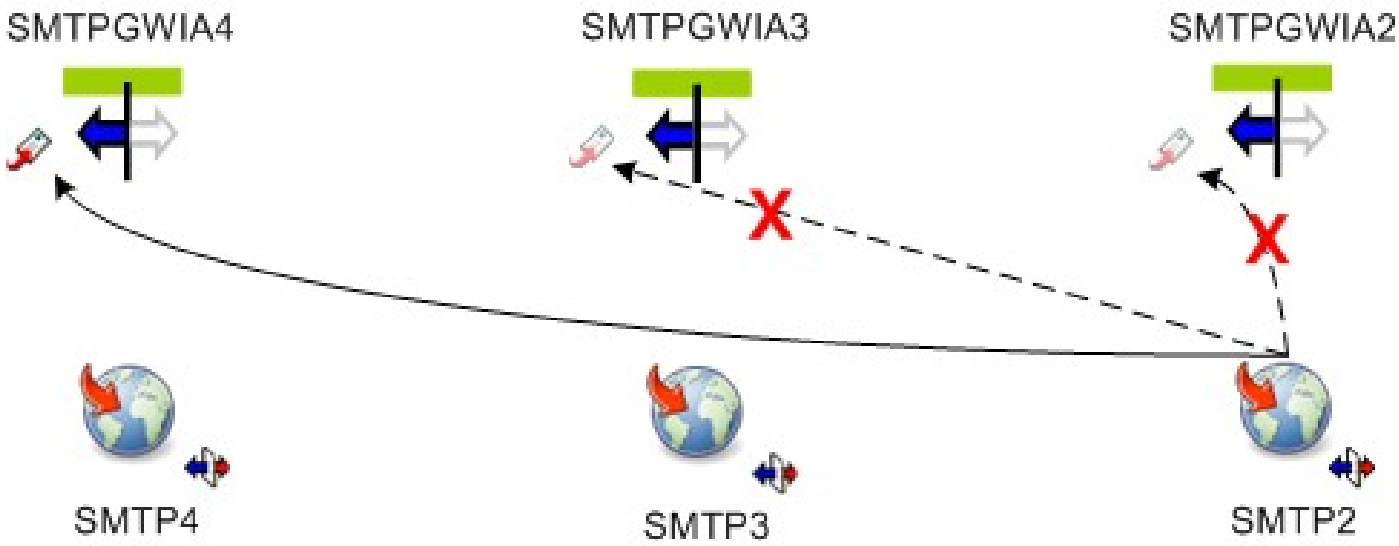
Redirection and Failover





Alternate Internet Agents: Gateway Chaining

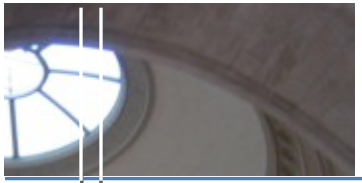
Redirection and Failover



Internet Agent for outbound SMTP/MIME messages:
SMTP4.SMTPGWIA4
Defined at: DVC_MAIL
Alternate Internet Agent for outbound SMTP/MIME messages:
SMTP5.SMTPGWIA5

Internet Agent for outbound SMTP/MIME messages:
SMTP3.SMTPGWIA3
Defined at: DVC_MAIL
Alternate Internet Agent for outbound SMTP/MIME messages:
SMTP4.SMTPGWIA4

Internet Agent for outbound SMTP/MIME messages:
SMTP2.SMTPGWIA2
Defined at: DVC_MAIL
Alternate Internet Agent for outbound SMTP/MIME messages:
SMTP3.SMTPGWIA3



GWIA Access Control

Connection ACL

SMTP Connection ACL's

Implementing "Restricted" Internet Agents

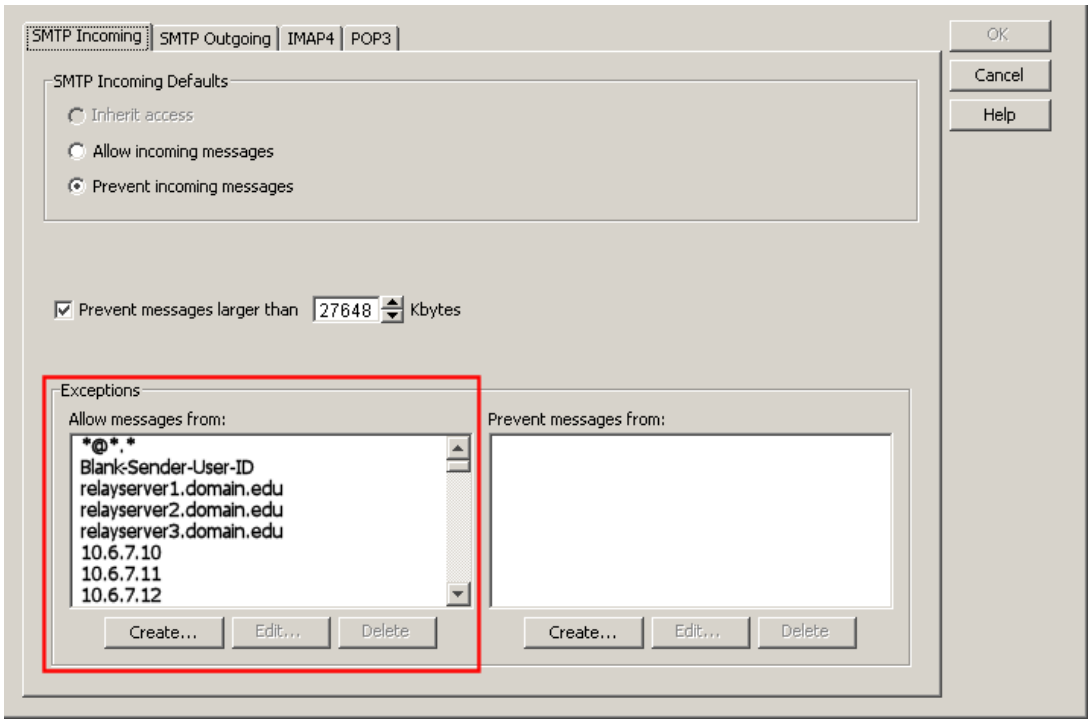
Use to limit **inbound** access to protocols and connections

Required exceptions:

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

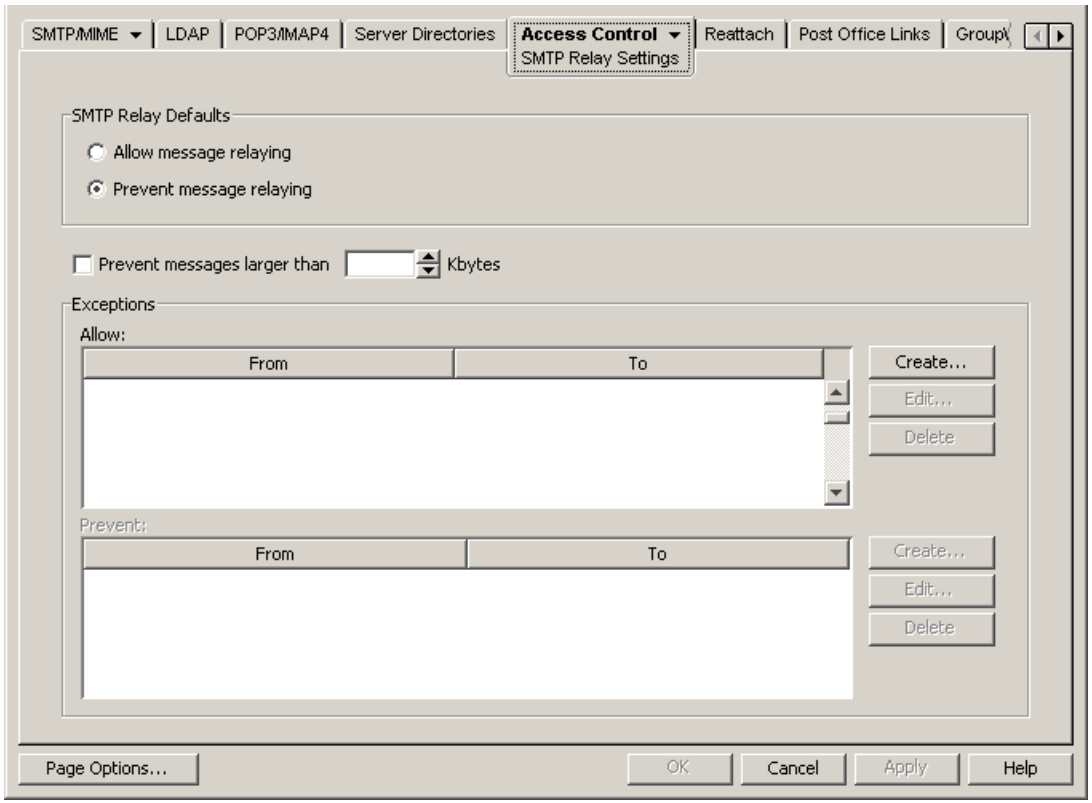
GWIA Access Control: Configuration

Connection ACL



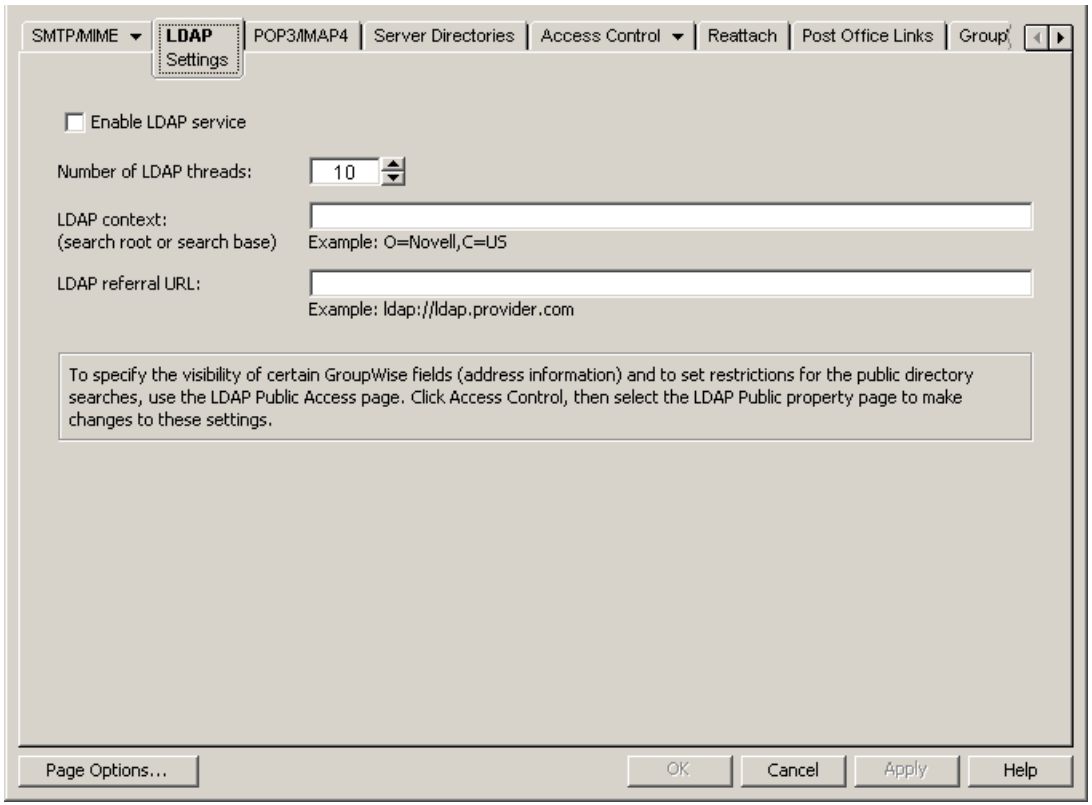
GWIA Access Control: Configuration

Relay ACL



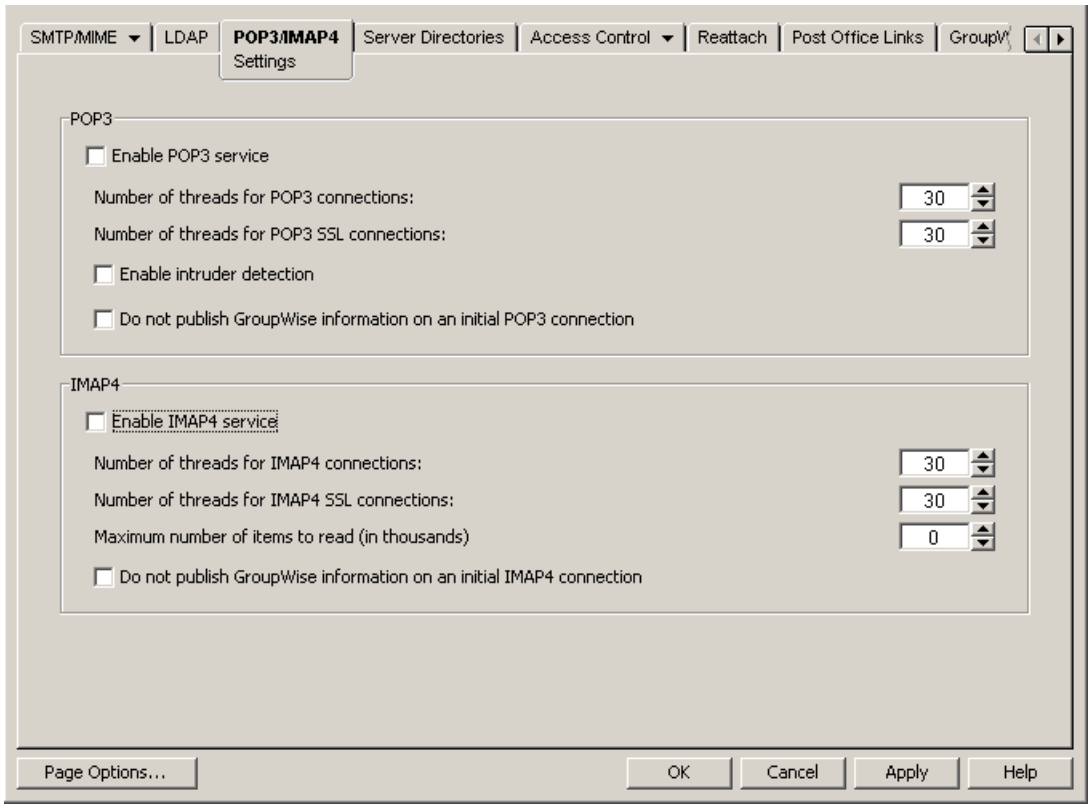
GWIA Access Control: Configuration

Connection ACL



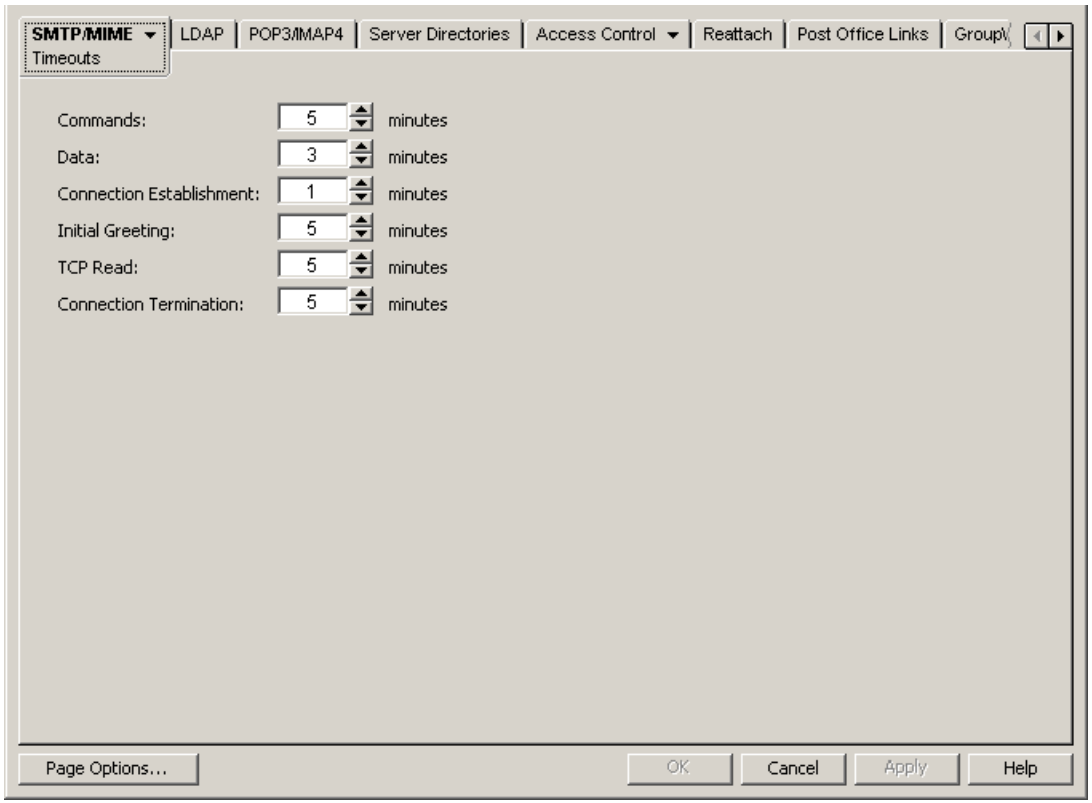
GWIA Access Control: Configuration

Connection ACL



GWIA Configuration: Configuration

Performance



System benchmark results

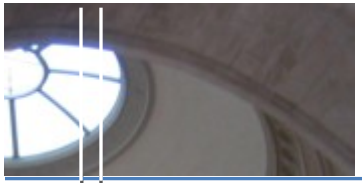
Performance

90 – 95% reduction in unwanted email at the perimeter

Quantifiable delivery performance increases

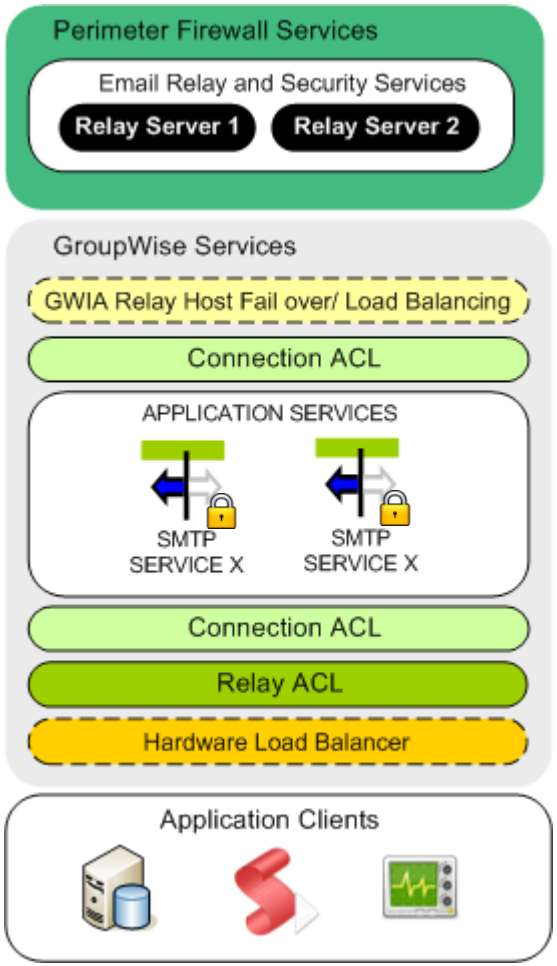
Unscheduled service downtime eliminated

Attachment sizes could be increased without performance penalties

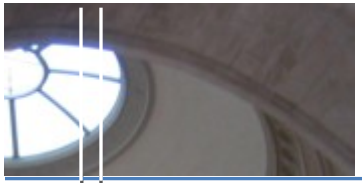


Services for Application clients

Services for application clients



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



SMTP services for unmanaged clients

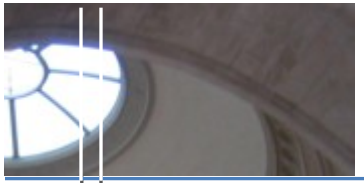
Security

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

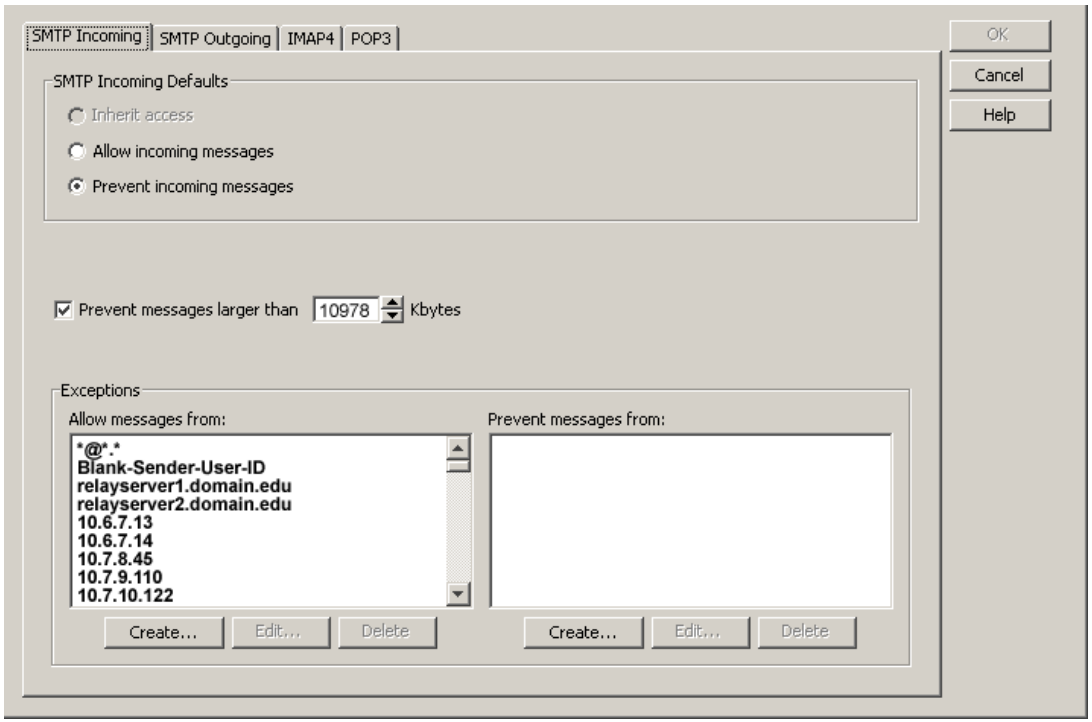
Anti-virus and malware infections

Cannot secure or audit third party “local” message stores

Cannot remotely manage or wipe unauthorized devices

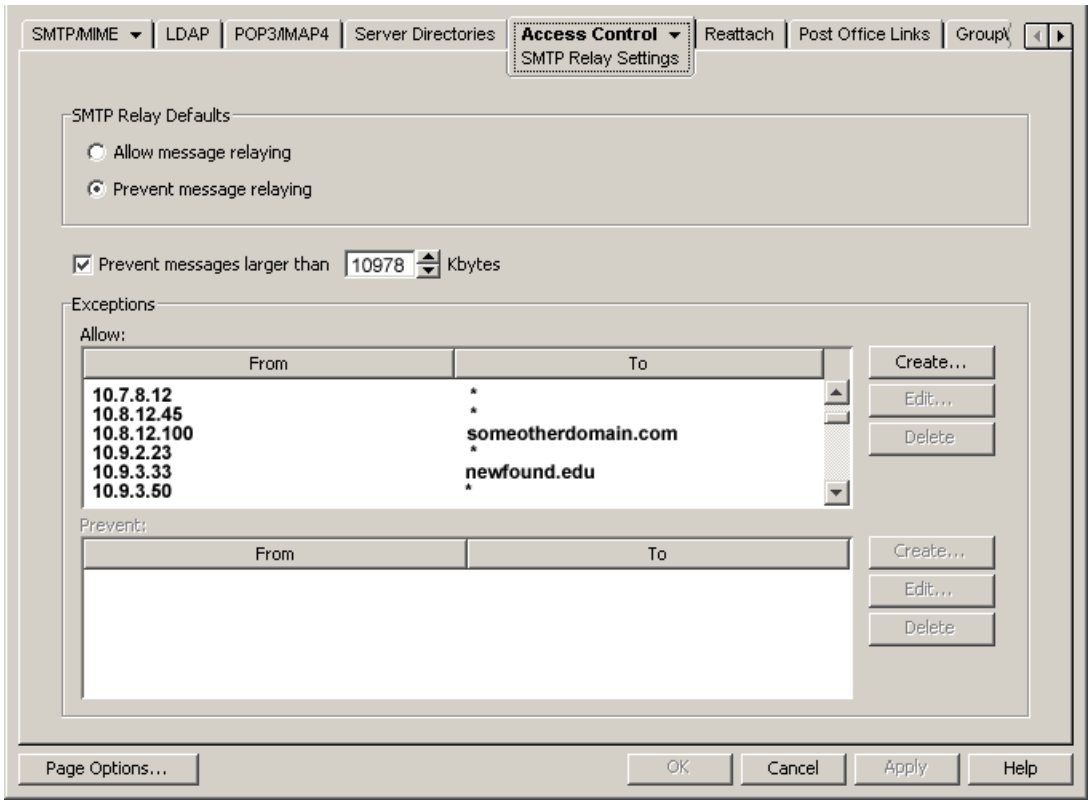
GWIA Access Control: Configuration

Connection ACL



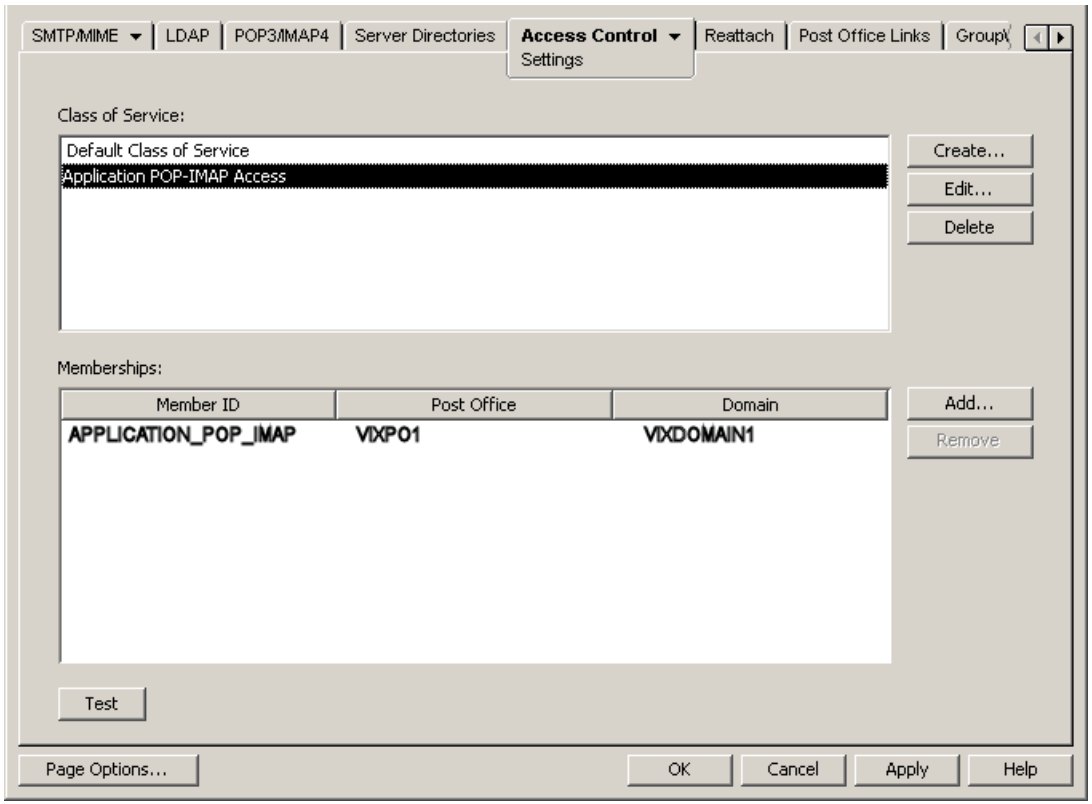
GWIA Access Control: Configuration

Relay ACL



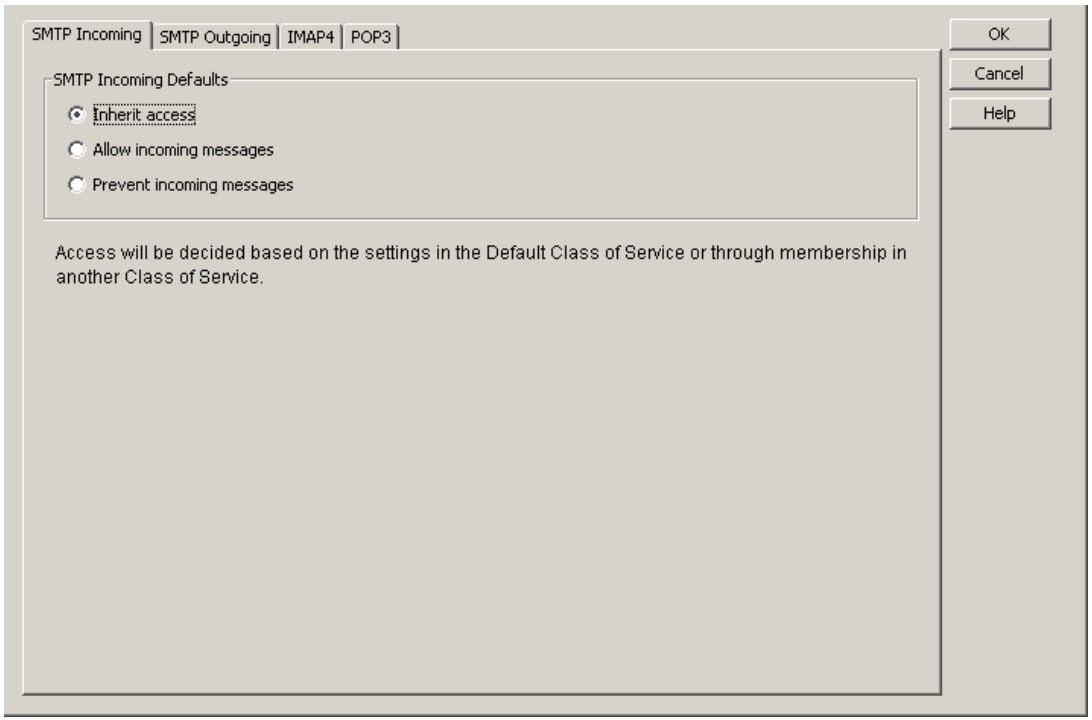
GWIA Access Control: Configuration

Connection ACL



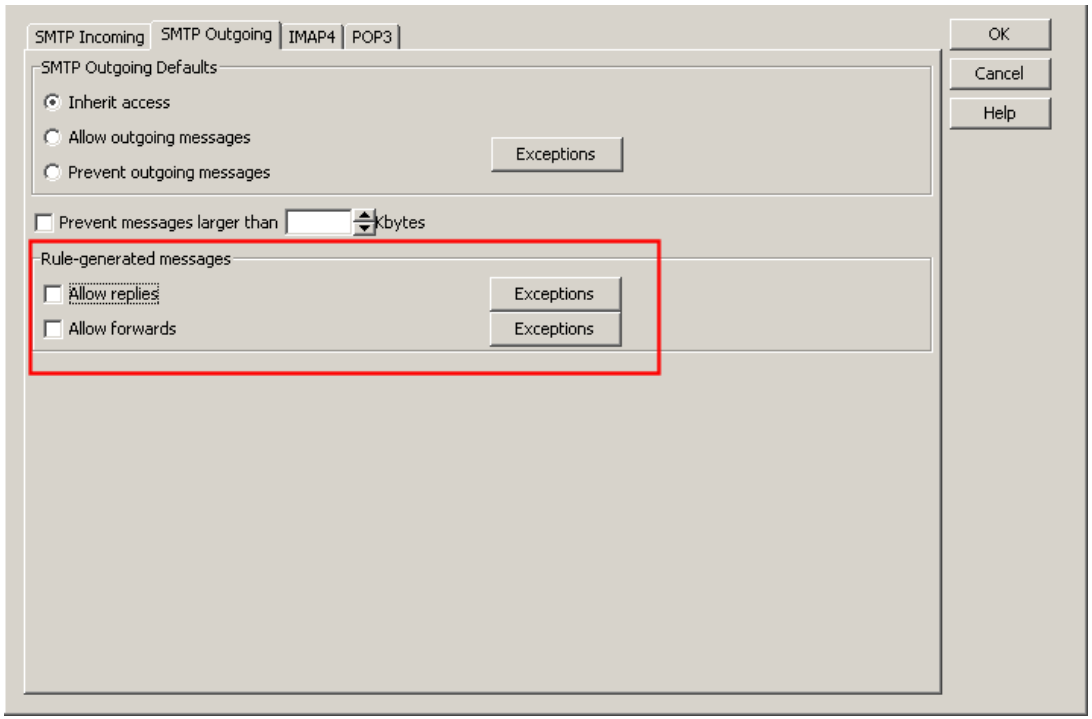
GWIA Access Control: Configuration

Connection ACL



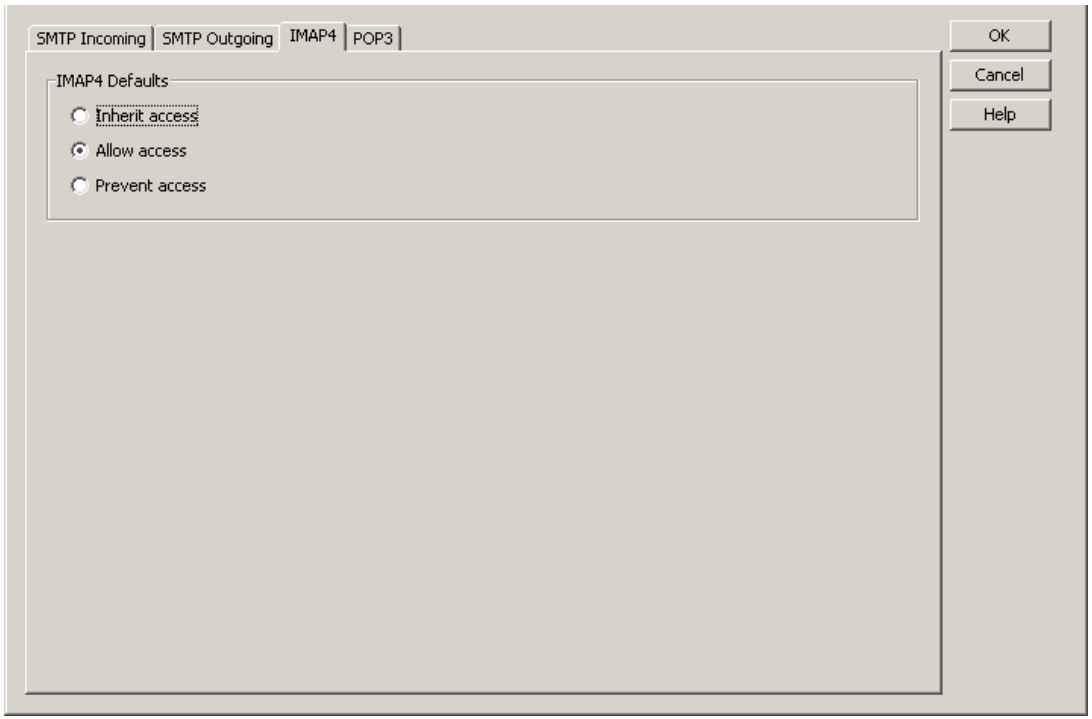
GWIA Access Control: Configuration

Connection ACL



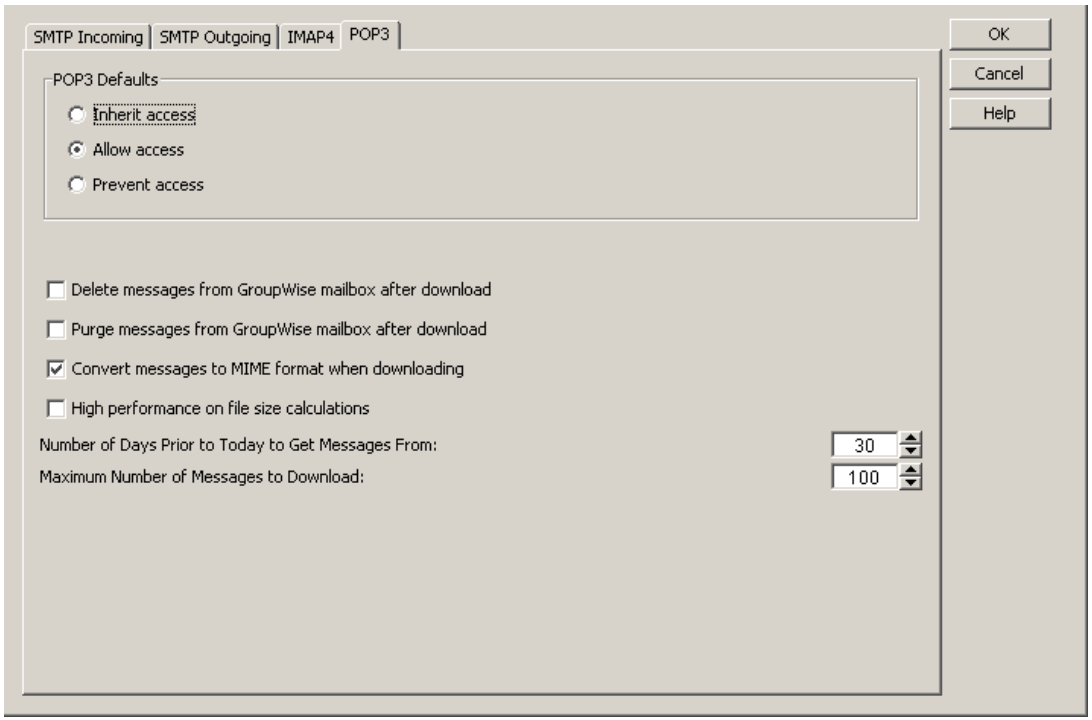
GWIA Access Control: Configuration

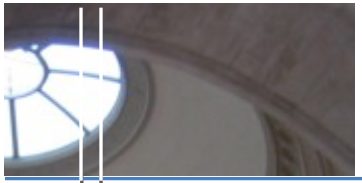
Connection ACL



GWIA Access Control: Configuration

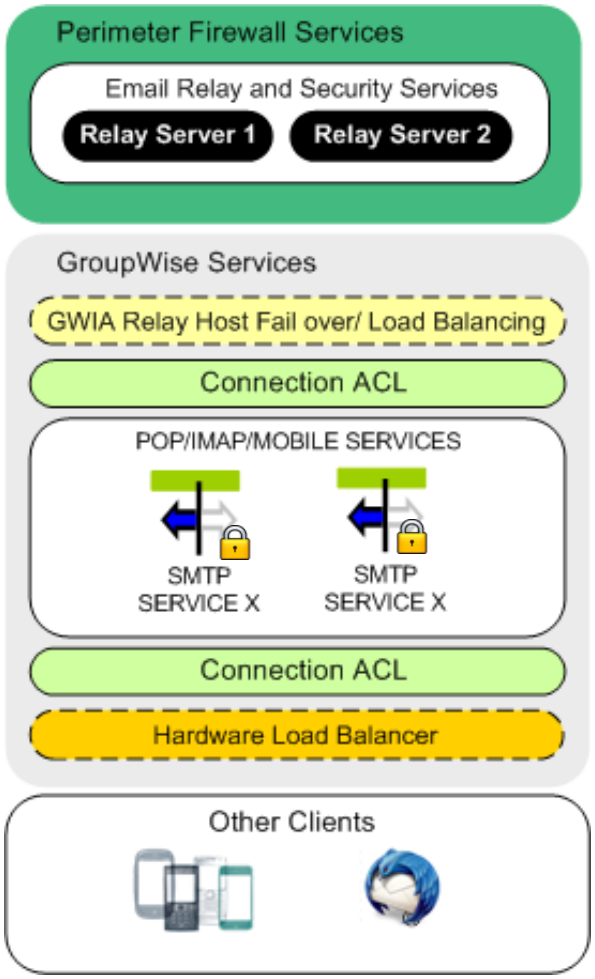
Connection ACL





Services for POP and IMAP clients

Services for POP/IMAP clients



Demarcations

Connection ACL

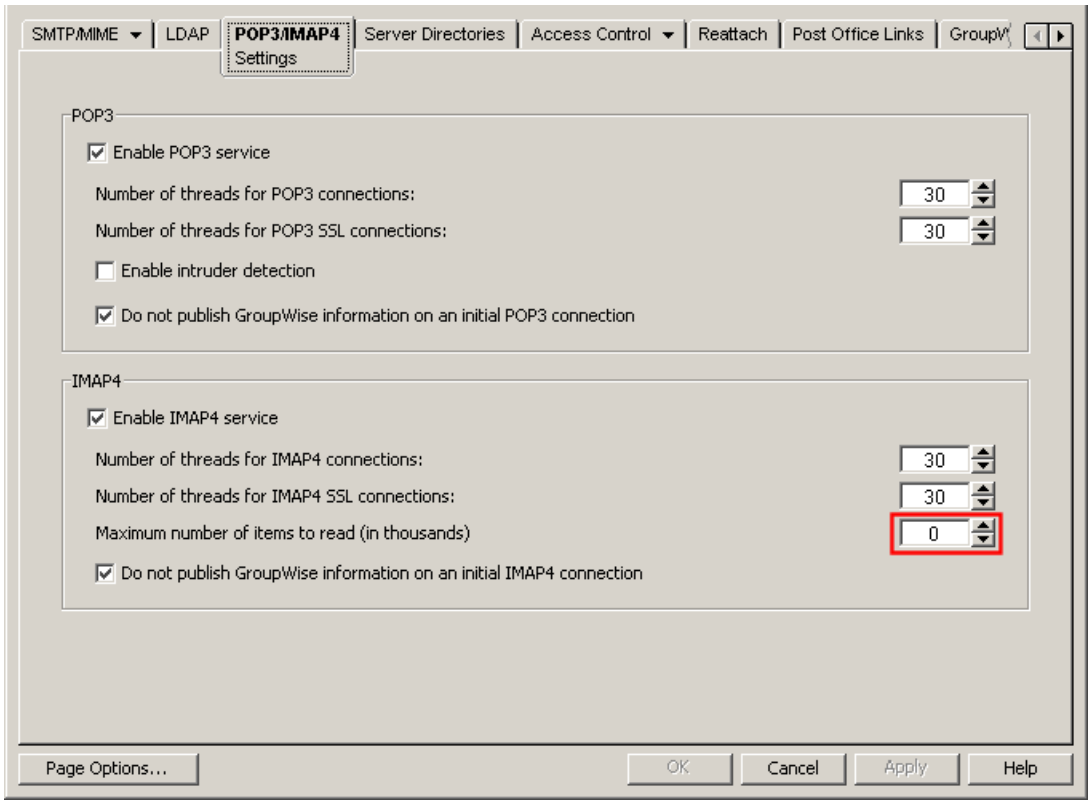
Software Load Balancing

Hardware Load Balancing

Performance

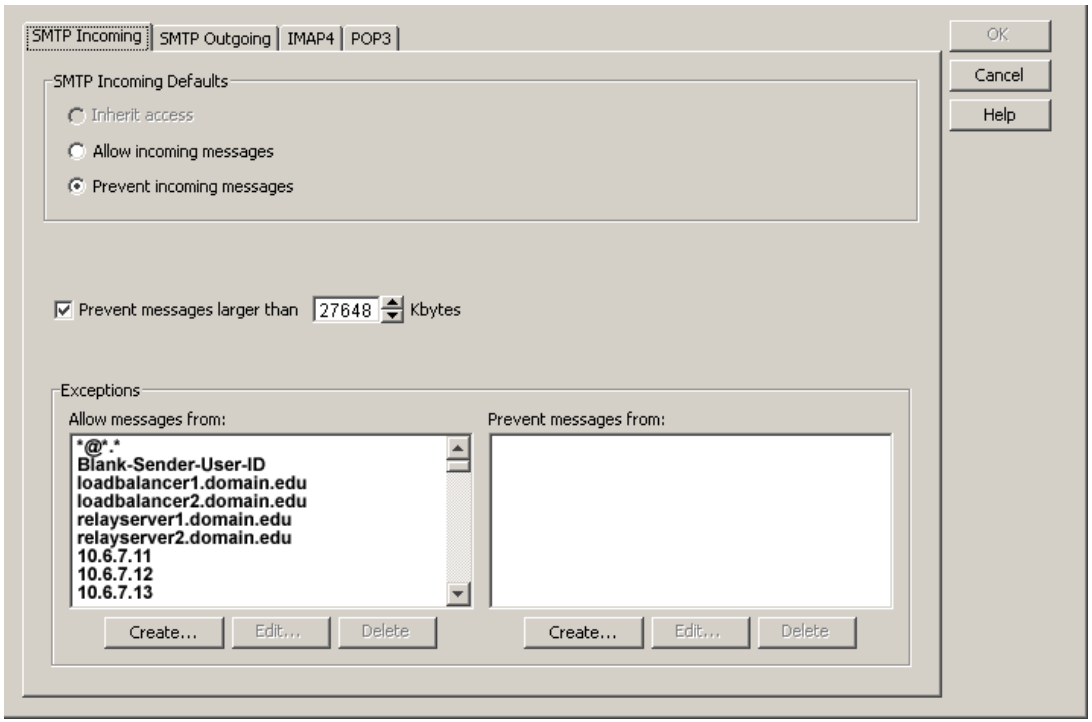
GWIA Access Control: Configuration

Connection ACL



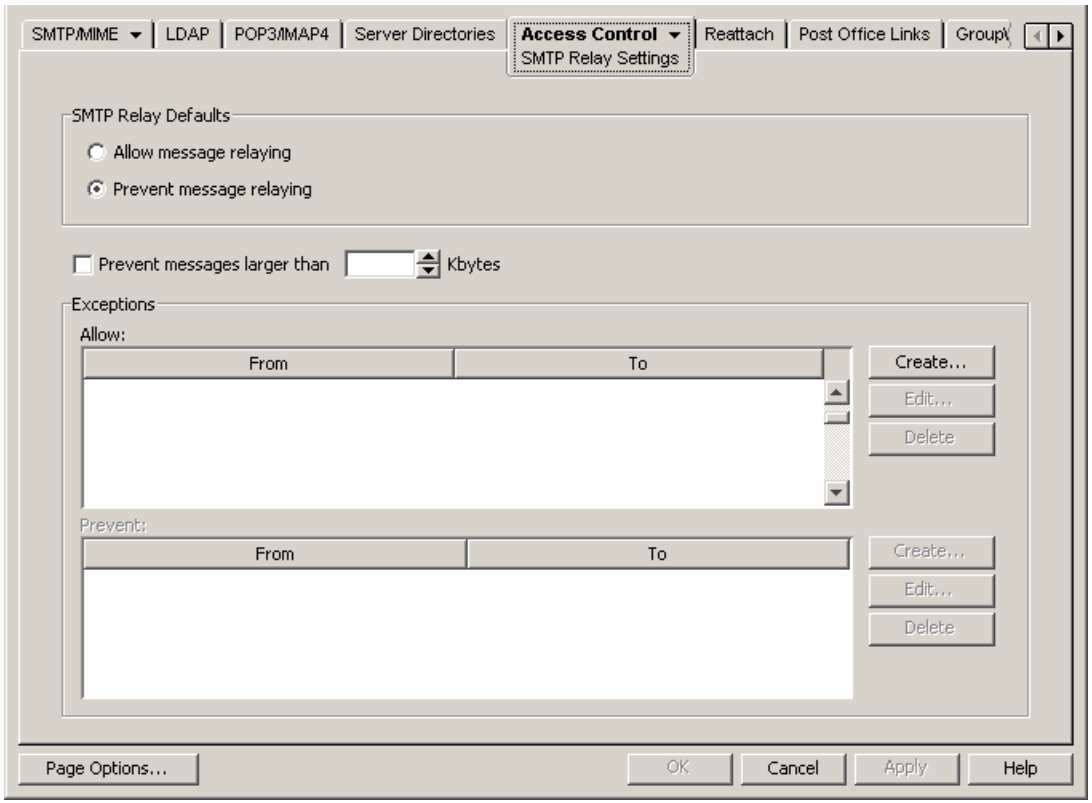
GWIA Access Control: Configuration

Connection ACL



GWIA Access Control: Configuration

Relay ACL



GWIA Access Control: Notes

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

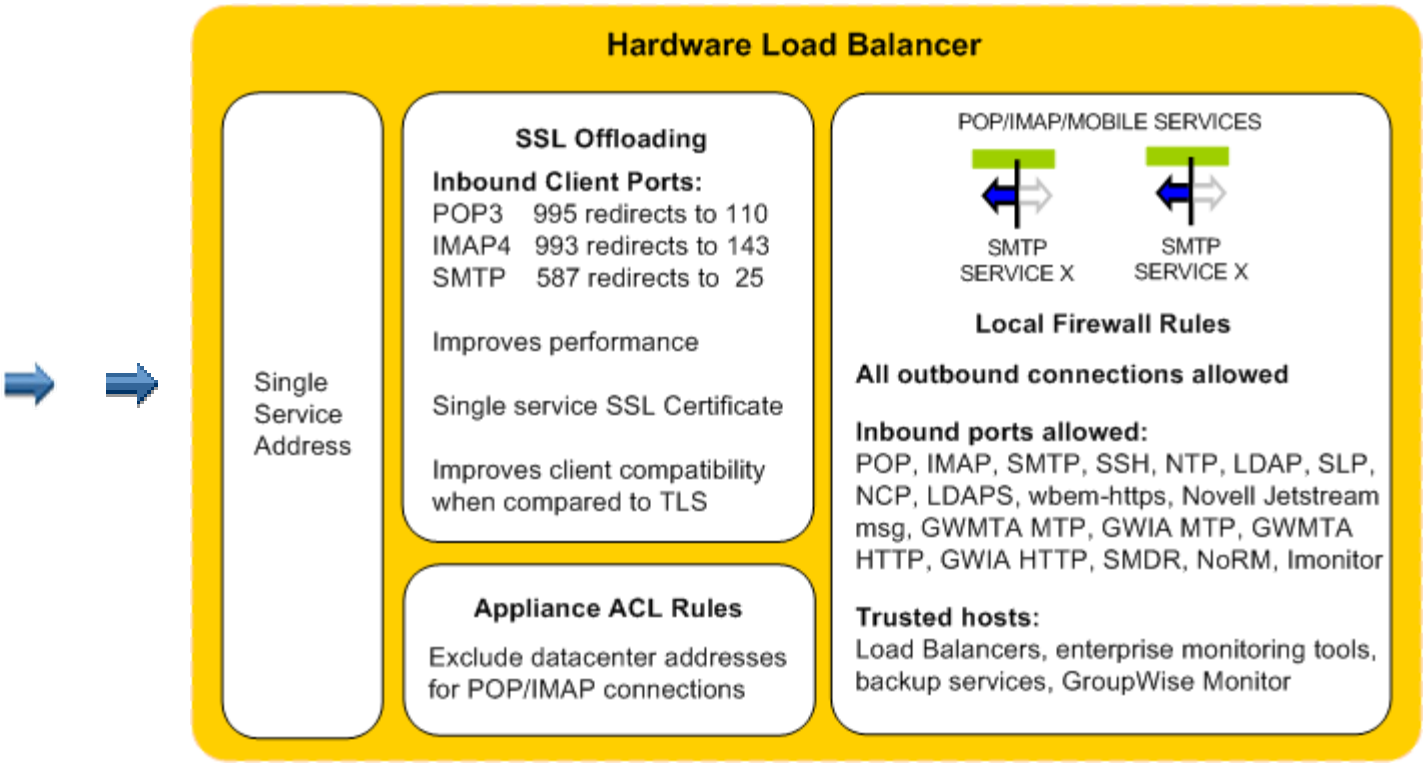
Relay Exception: someiDomain.com

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

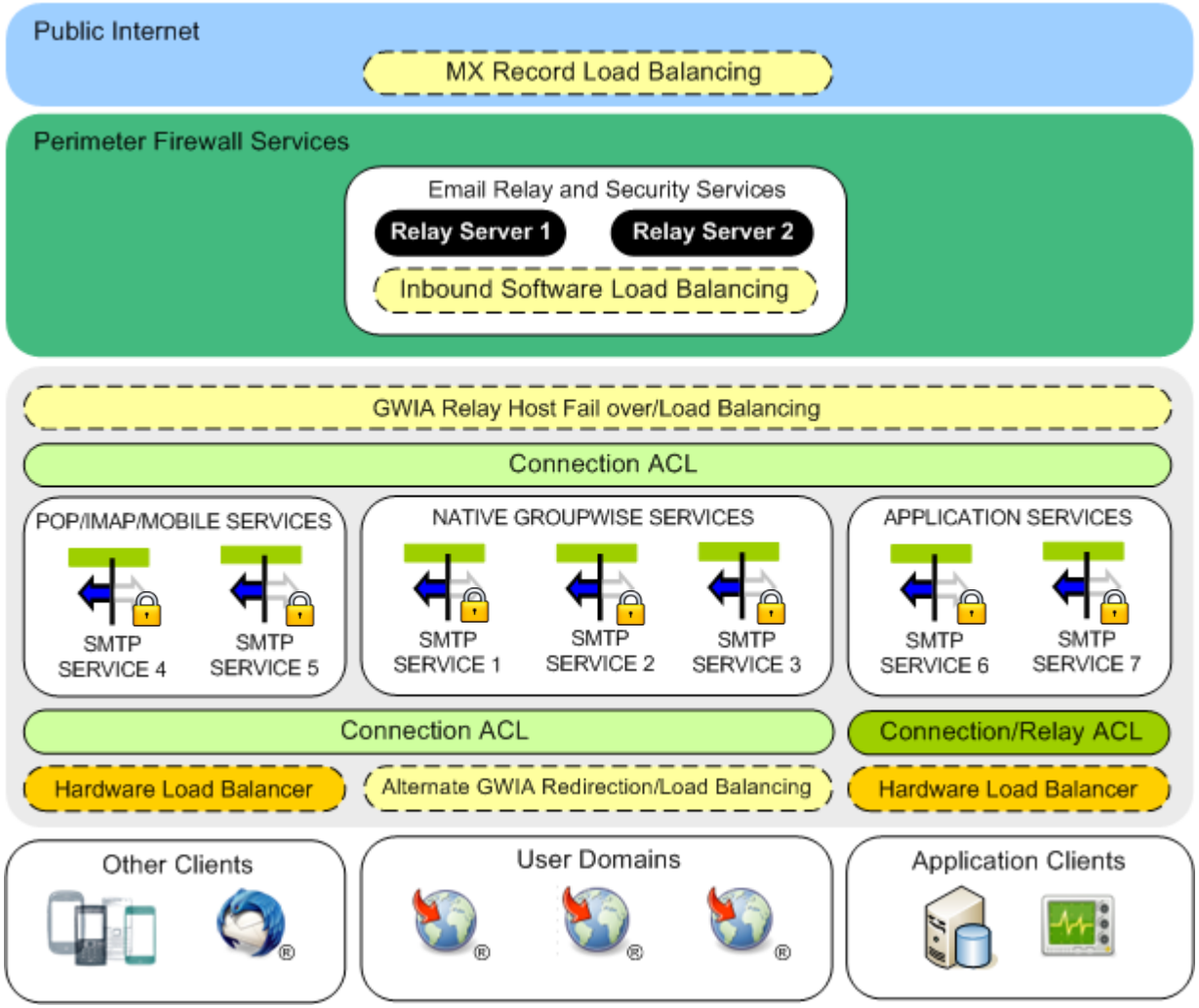
The /etc/SuSEconfig/SuSEfirewall2 configuration file:

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"

Bringing it all together

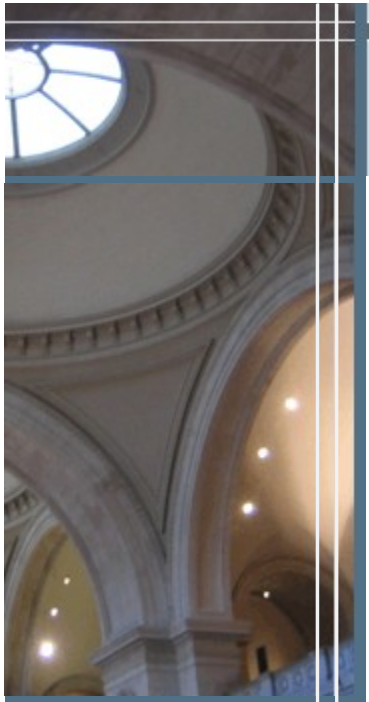


Technical and configuration details

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 !