# GroupWise SMTP infrastructure design

**Lawrence Kearney**
Enterprise and Work Group Service Analyst
Georgia Health Sciences University
lawrence.kearney@earthlink.net

TTP (EMEA) July 2011

Novell®

# Session description

- A meaningful discussion on email service trends and the architecture developed in response to them
- Viable third party security , traffic fencing, and traffic shaping options are referenced
- Most information is geared for large and enterprise size environments
- Designing and maintaining systems to align with similar commercial service offerings

# Presenter description

- Have been administering GroupWise since version 4
- Have a knack for destroying thumb drives and glassware
- Have learned to like Linux
- Have just recently learned to use flatware properly
- I like to help

# Why design SMTP infrastructures

- Provide an operational profile of your SMTP services
- True optimisation can only occur when service usage patterns are laid bare
- To increase the performance and features available to users
- Information gleaned before and after can be used for auditing, monitoring, and scaling
- To provide your organization with an improved and reliable mission critical service

# Some service benchmarks

- Service performance
- Service efficiency
- Service stability
- Service feature sets
- Service cost of ownership
- Service planning and scaling
- Service standards

Influences leadership, staff, and customer "**dissatisfaction**"

# What can we do to improve services?

- Clever architecture and design choices
- Service access control and redirection
- Service load balancing/management
- Service redundancy/high availability
- Service I/O fencing and demarcations (QoS really)

Using blended solutions can provide a basic business policy framework for your service

- Managed network architecture
- Application traffic management
- Business policy enforcement

# Clever choice: Using Relay Servers

Benefits

- Additional layer of abstraction and obscurity
- I/O isolation and management
- Alternate access control point
- Addition of non-native features and services

Caveats

- Additional complexity

# Using Relay Servers

**The trouble with relays**

External relays: Functional (Blacklisting etc.)

Internal Relays: Functional, Administrative

Windows Relays: Usually in a differing AD domain

Single App Hosts: Use Network Address exceptions

Multi-App Hosts: Use Fully Qualified Email Address (FQEA) exceptions **

** Feature enhancement request needed

# Clever choice: Using ACLs

Benefits

- Prevention of unauthorized access to services
  - OMG … if you just checked those logs
  - Internal misuse and security compliance issues
- Service demarcations (QoS really)

Caveats

- Additional complexity
- Difficult to implement in existing environments
- Additional management overhead

# Using ACLs

GroupWise specific ACL requirements

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

If these aren't in your GWIA Class of Service configurations you'll get disappointing results

Use Class of Service capabilities to make ACLs global, granular and modular

# Using ACLs

Relay logic truth tables will help with your ACL implementation

**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: "yourdomain.edu"**

| 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 |

# Clever choice: Using Load Balancing

Types: Hardware, software, native, blended

Benefits

- Managing multiple agent instances to “implement” a service
- Access control aggregation
- SSL certificate aggregation
- Service performance improvements
- Addition of non-native features and services
- More compatible service security using SSL

Caveats

- Additional complexity

# Clever choice: Using Clustering Services

Types: Novell Clustering Services and Linux High Availability

Benefits

- Improves service redundancy options
- Improves service high availability options

Both are very cost effective options that allow you to scale up

Caveats

- Additional complexity

(Virtualisation can compete here but with additional cost and overhead)

# Clever choice: Internal human resources

Leadership

- Support greatly improves your chances for success

(Find clever ways to secure it)

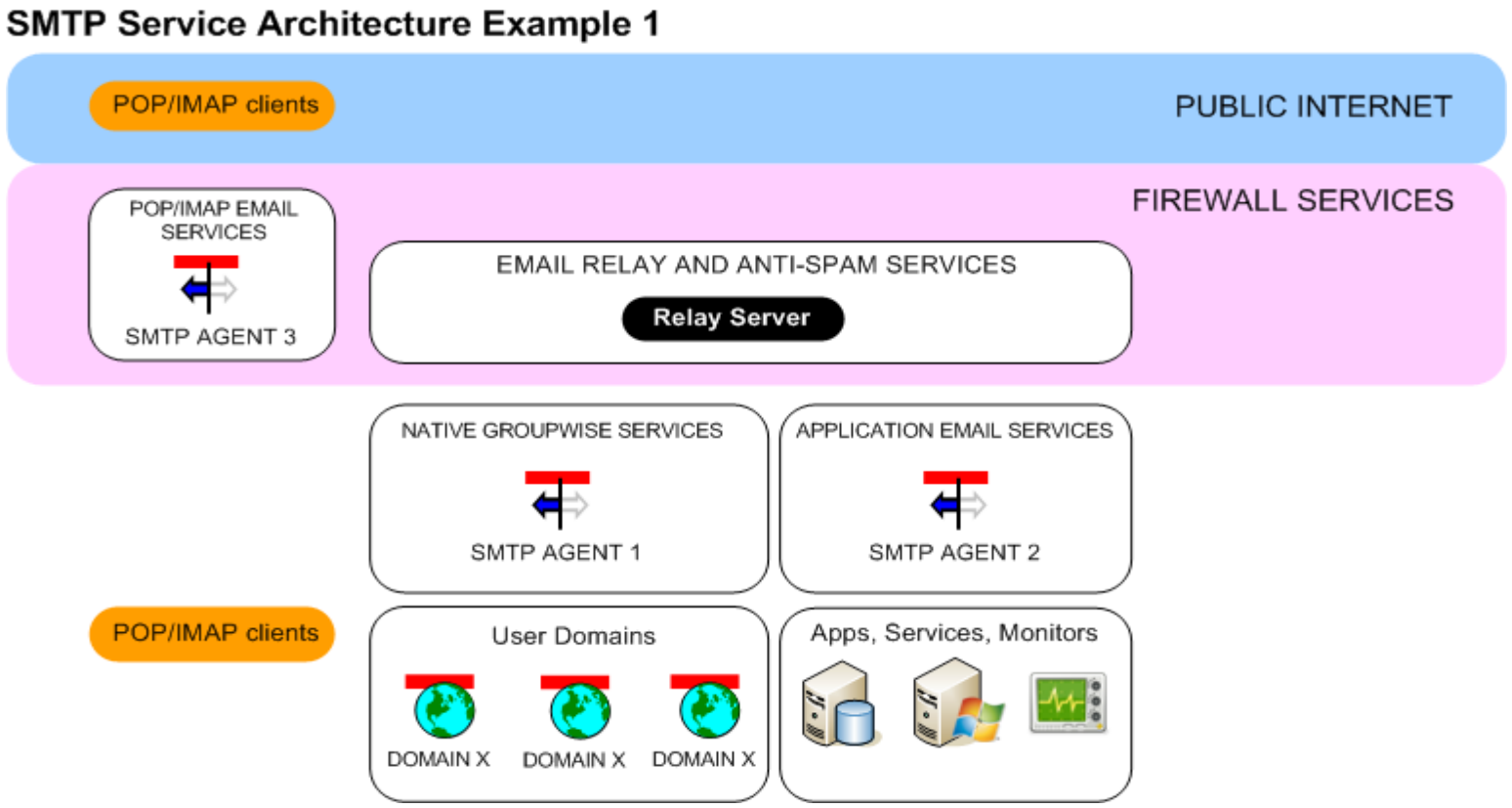
Infrastructure

- Partner with other departments to develop new business processes and procedures to ensure the supportability of solutions

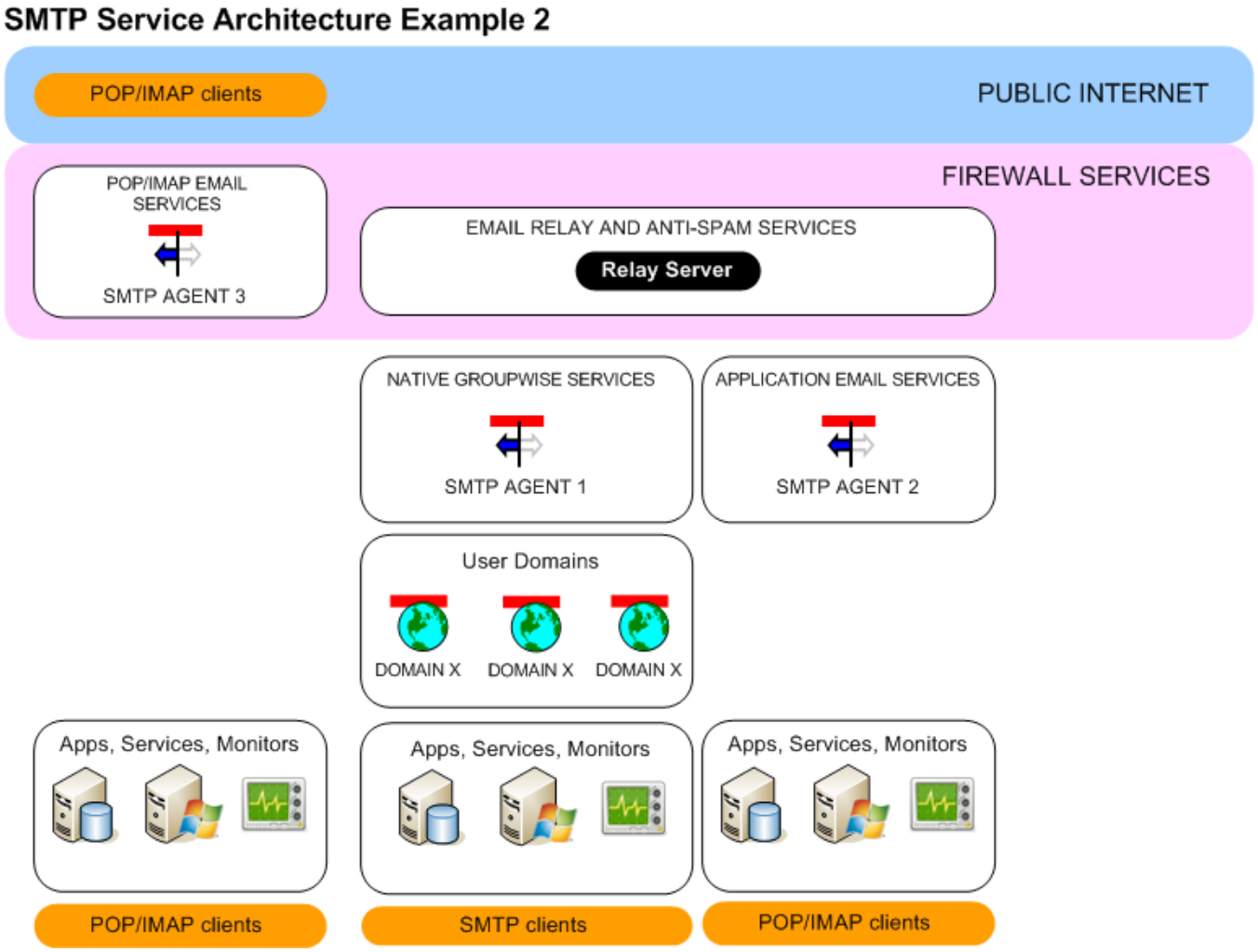
Support

- Work within your organisation to advocate, document and support procedures for internal staff

# Learning to peel back the onion



# The best laid plans of mice and men ...



# GroupWise POP/IMAP service issues

- **Unmanaged desktop and device clients**
  - Fat and thin clients
  - Device clients (Email “Scourge”)

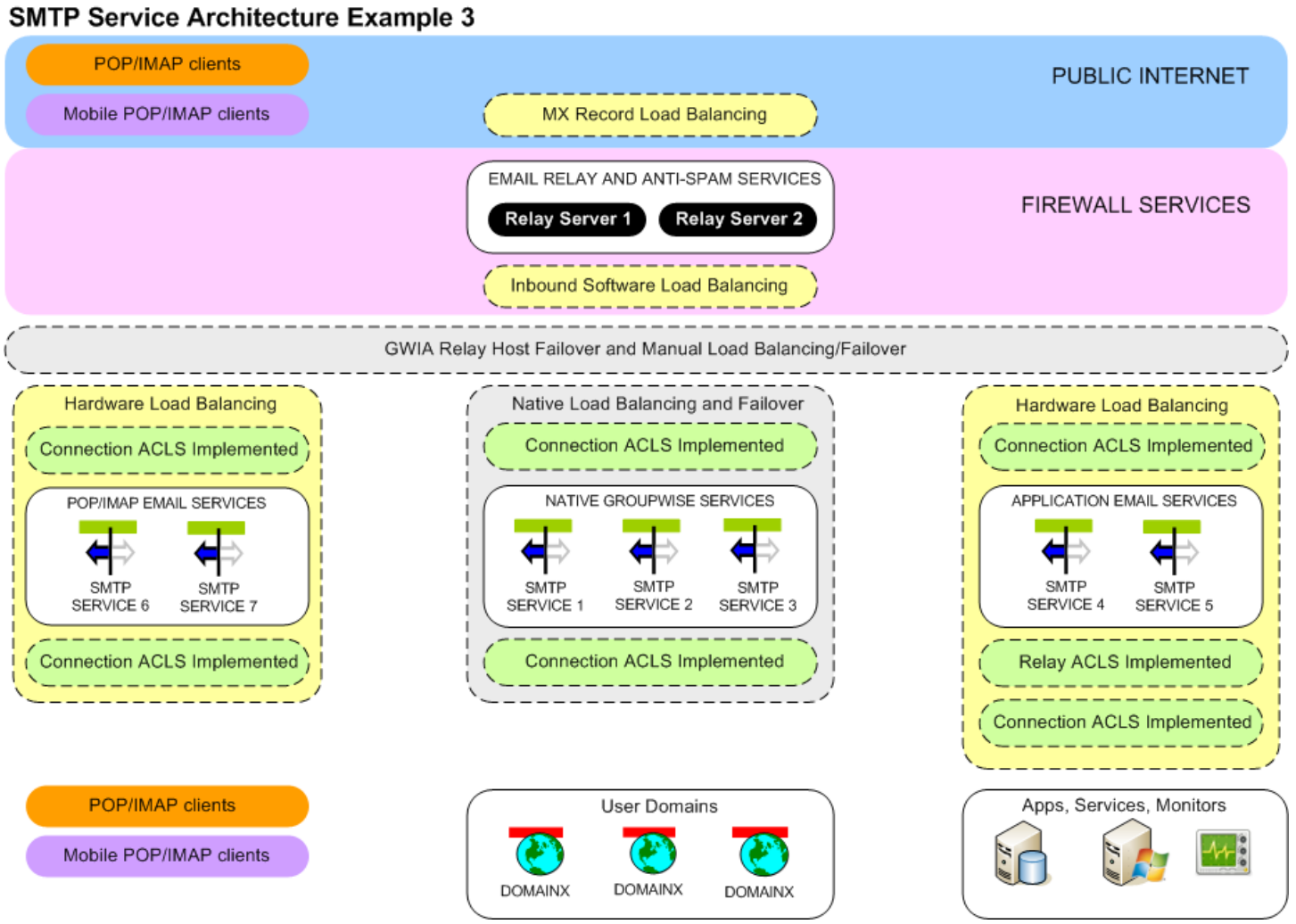
  **Scourge**: a person or thing that administers or applies punishment or severe criticism

- **Additional security concerns**
  - Encrypted connection issues (really the lack of)
  - Cannot secure third party “local” message and credential stores
  - Cannot remotely manage or wipe unauthorized devices

# GroupWise POP/IMAP service issues

- Additional support footprint
- Bandwidth overconsumption
- Loss of managed client features
- Service providers “consuming” GroupWise services
  - BIS
  - mMode (mymmode)
  - Notify Link

# A new service design



# Service architecture decisions

## GroupWise Internet Agents

- Native GroupWise ACLs are applied
- Agents are chained for fail over
- Multiple mail relay targets used
- Never allow “true” open relay configurations
- Load balanced wherever possible

## Gateway domains

- No regular users live here

# Continuing with the theme ...

**User  post offices**

- No direct POP/IMAP connectivity to POAs

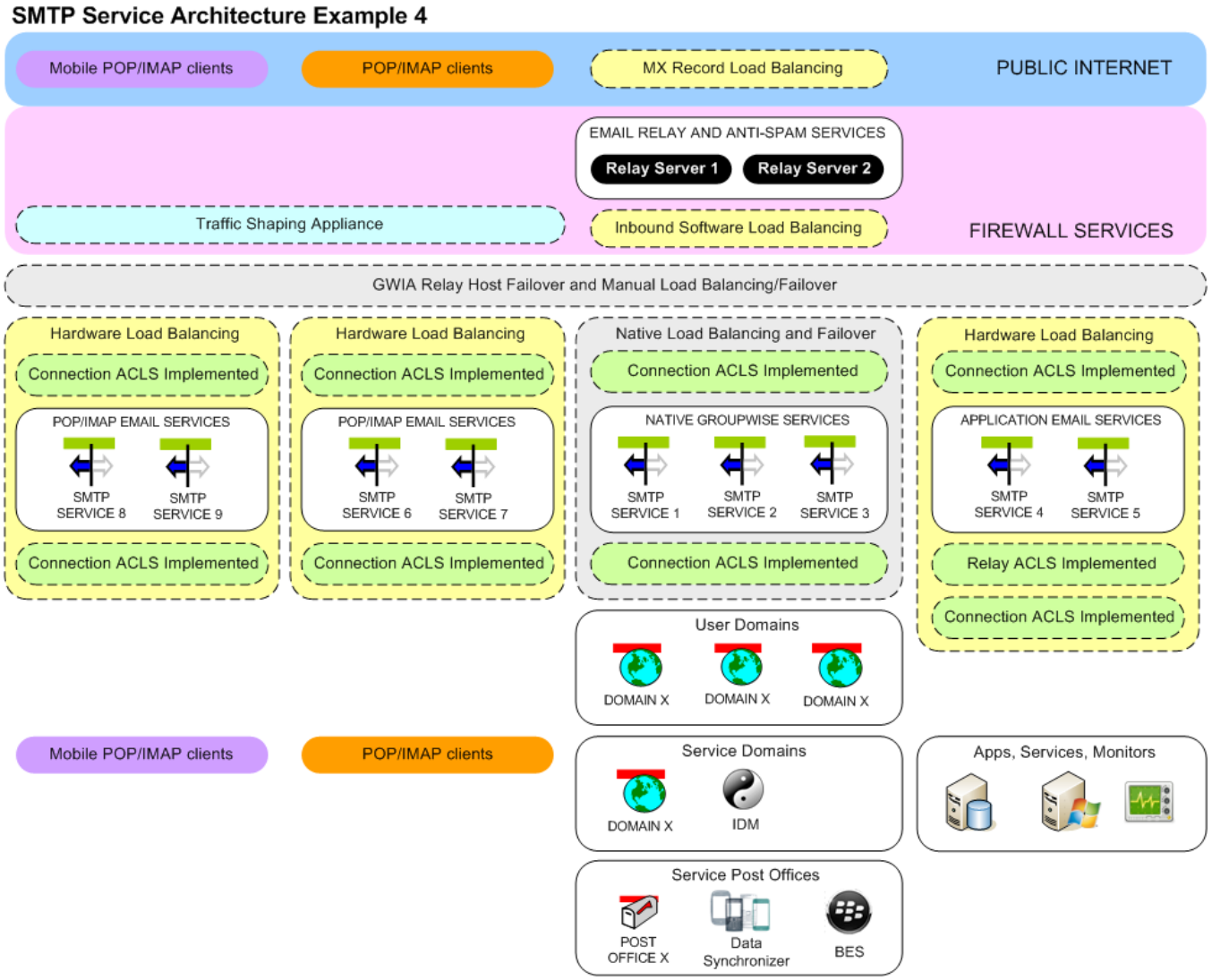
**Service domains**

- IDM services connect here
- Are not parents to gateways or post offices

**Service post offices**

- No regular users live here
- Managed third party client ingress points
- Application and service accounts

# A newer service design



# So what do we get if we consider this stuff?

- Service performance improvements
- Service availability improvements
- Service capacity monitoring improvements
- Service capacity management improvements
- Service feature set expansions

Influences leadership, staff, and customer "**satisfaction**"

# Best Practices

Routing undeliverable messages

- All messages should go somewhere
- Service and application accounts should have an in box
- Return paths for bounces and relay denials
- You may want to audit or assess undeliverable messages
- Prevention of message acceptance/response loads on relay servers

# Best Practices

GWIA switches

- Use the **/realmailfrom** switch or the "Use GroupWise user address as mail from" ConsoleOne setting to prevent rule based forwards from being sent out as being from the postmaster

- Use the **/forceoutboundauth** switch for GWIAs dedicated to third party client use

IDM

Use the remote loader for domains hosted on Linux. IDM drivers using NCP can introduce file ownership and case issues for the admin messages they create in agent queues.

# Best Practices

Security configuration

- Be careful and test SMTP inspects implemented by security devices and services
  - Firewalls
  - Intrusion Prevention Services
  - Relay Servers

Some can be “MIME mungers”

- Implement Sender Policy Framework (SPF type 99) DNS records for your organization

# Troubleshooting

SMTP service management and assessment tools

- http://www.dnsbl.info/dnsbl-database-check.php
- http://www.mxtoolbox.com

- Using **netstat -patune | grep ':25'** command to assess connections to your Linux hosted GWIAs

POP/IMAP account testing

- Let GW Monitor populate a test account for large in box genre testing needs


Novell®