SENDMAIL®

Future of Anti-Spam Defence

The Combination of Sender Authentication and Content Filters

Internetdagarna, Stockholm 1 November 2004

Thorgeir Einarsson
Managing Director EMEA – Sendmail Inc.

Agenda

- Sendmail Profile
- Key Anti-Spam Trends
  - Drilldown on Sender Authentication
- Internet Email Issues
  - Security
  - Compliance and Control
  - 24 x 7 availability and reliability
- Solutions
  - Total Email Management
- Summary

Who is Sendmail ?

SENDMAIL®

Founded in 1998 – Headquarters in Emeryville, CA

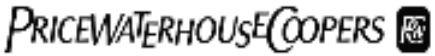
- Offices in North America, Europe and Asia
- Pioneered internet email routing with SMTP
  - Setting new email standards with partners - Sender Authentication
- Leading total email security and content mgt
  - 60% of all internet email uses Sendmail
  - 7 out of 10 Fortune 100 use Sendmail

What exactly do we do.....?

SENDMAIL®

Sendmail Delivers

- The most comprehensive solutions and services for security, control and management of email
- Cost-effective large scale mailbox servers
- Leverage our open source experience to drive new email standards

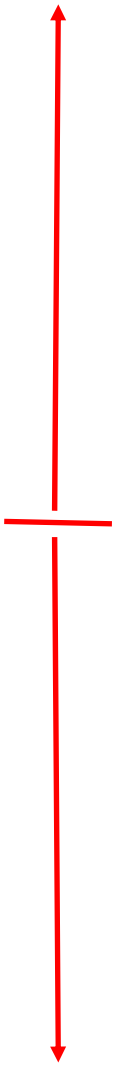


SENDMAIL.NET

Issues Breakdown

SENDMAIL®

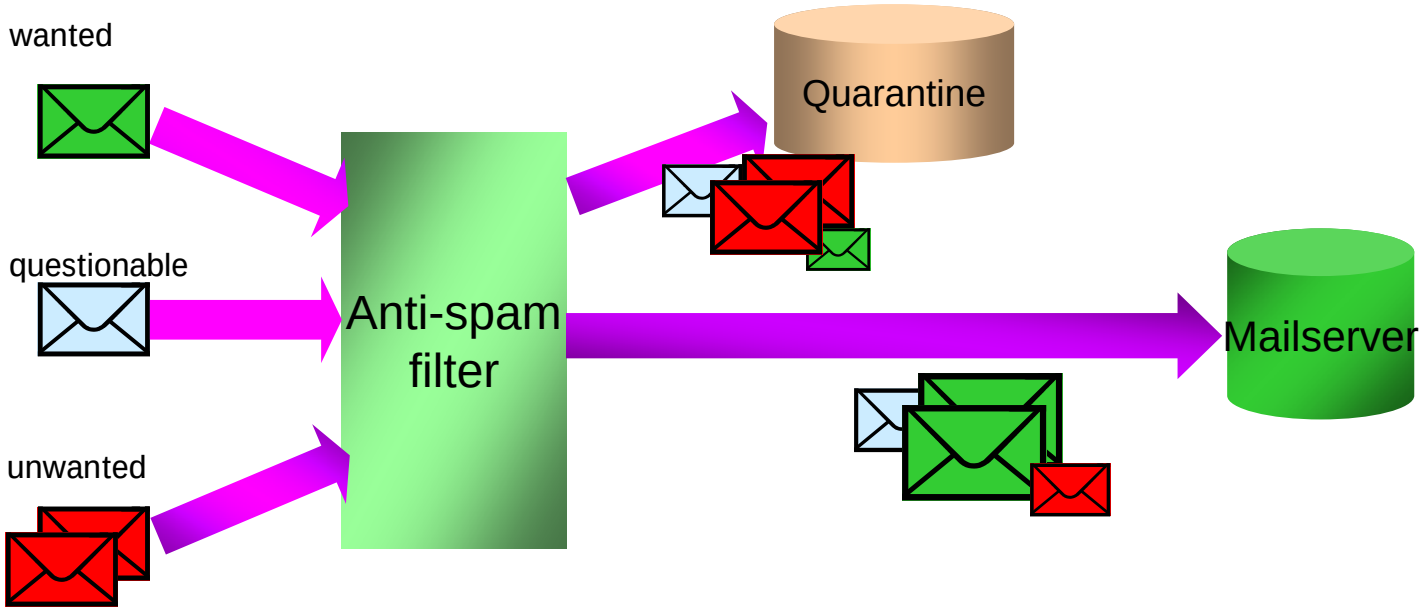
Management
Message Store
Growth
Security
Archiving/ Retention



- **Spam**
- Growth in messaging storage
- Increasing employee use of attachments
- Viruses, worms, Trojan horses, etc.
- Users sending large attachments through email
- Managing remote users
- Users complaining about mailbox quotas
- **Users sending and receiving inappropriate content**
- **Employees' personal use of email**
- Finding message content older than 12 months
- **Users sending confidential data improperly**
- Finding message content older than 6 months
- Finding message content older than 3 months
- Denial-of-Service attacks

Source: "Enterprise Messaging Systems: Market Problem, Needs and Trends", Osterman Research, 2004

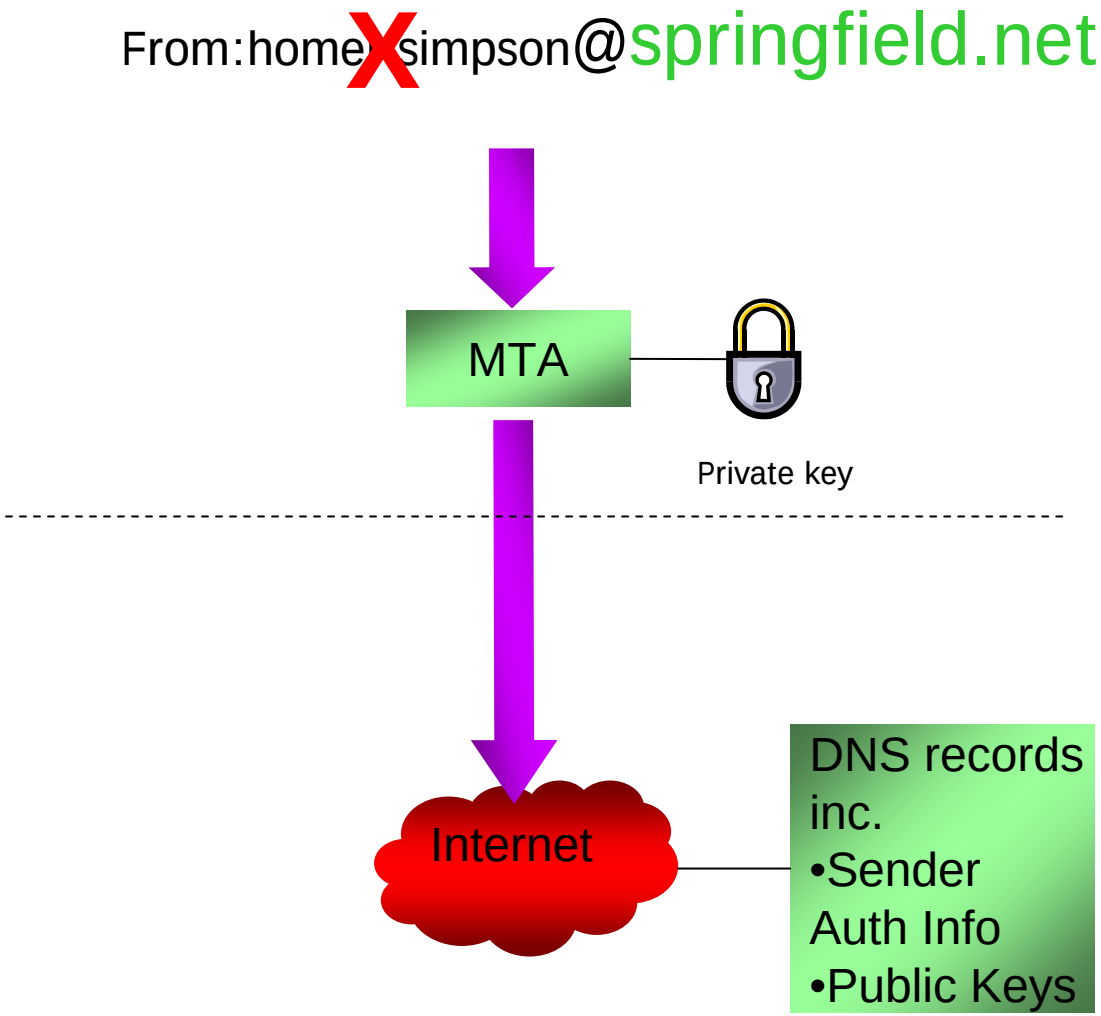
Current Email Infrastructure is threatened....



- System based on implicit trust does not scale to **half a billion** of users
- Need new standards to address this – **Sender Auth**
- Filters alone cannot stem the tide of SPAM / Email fraud

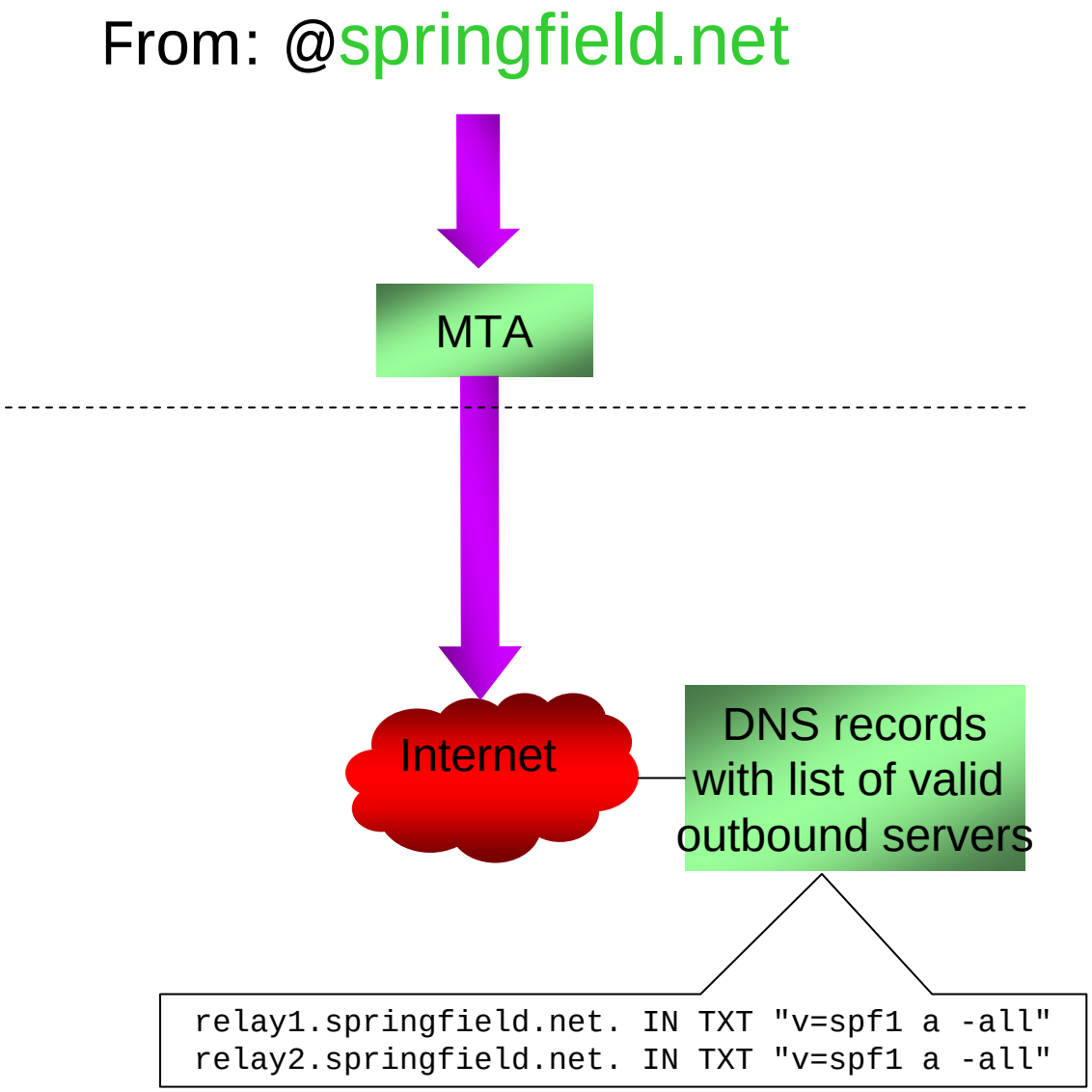
What is Sender Authentication

- NOT identity
- We want to “Prove” authority to use a domain
- Two general strategies are being pursued
  - IP based
  - Digital Signatures
- Sendmail is committed to support ALL schemes that work and have adoption
  - We have SPF, SIDF and DK today



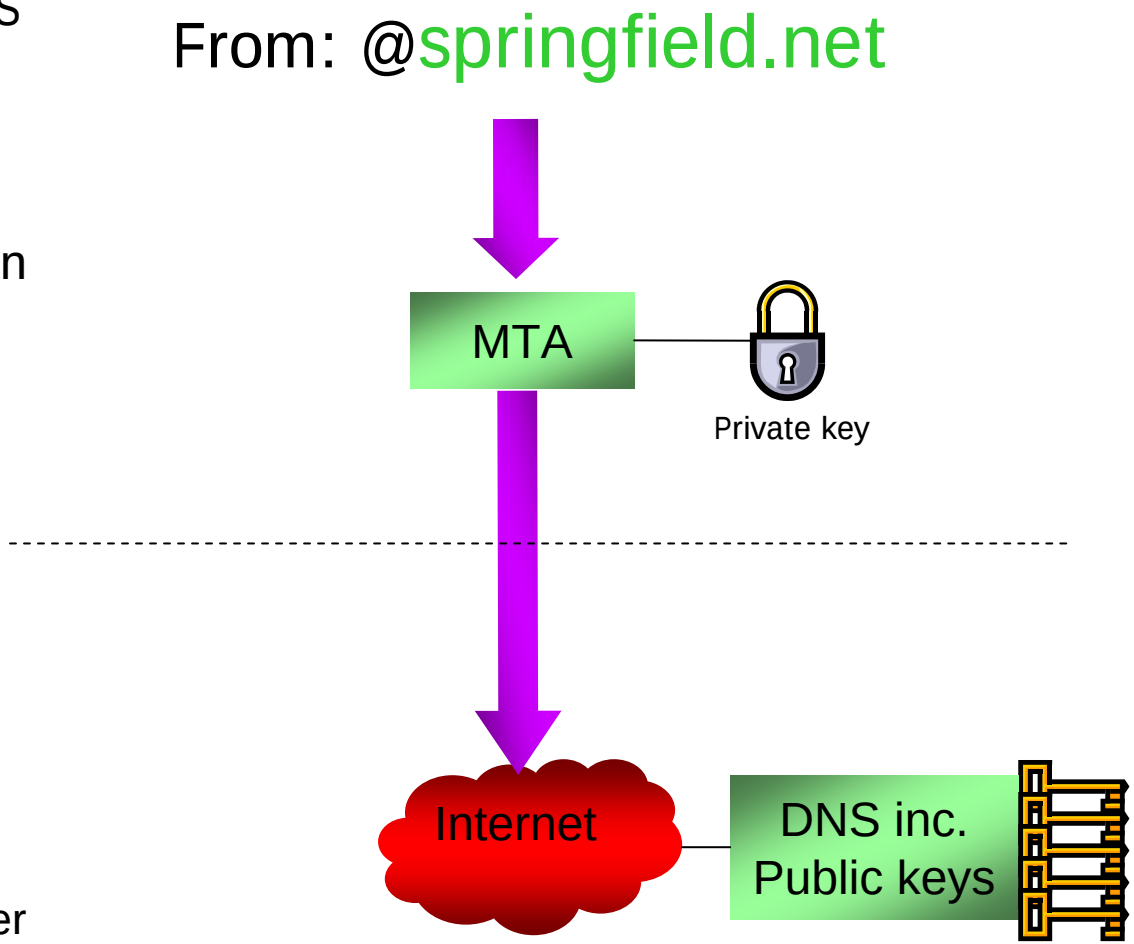
Sender ID (SPF, SIDF)

- IP addresses of domain mail servers are stored in DNS TXT records
  - Senders do no additional work
- Receiver picks up IP list from DNS and verifies the sender IP
  - Authenticates the last hop
  - Has some forwarding problems
- Trivial for the Sender to deploy



Digital Signatures: Yahoo DomainKeys

- Public keys are stored in DNS TXT records
- Senders Sign Messages with Private key & put signature in the header
  - Signature protects headers and content
  - Authenticates domain only
  - Selectors provide key management
- Receiver picks up public key from DNS and verifies the signature
  - Authenticates original sender
  - No forwarding problems



Authentication Comparison

- IP based (Sender ID)
- Publish out IPs in DNS
- Receiver verifies IP
- Last IP is authenticated – May not be Sender
- Forwarders & mail lists must change
- Much easier for senders to deploy
- Tough on forwarders

- Digital Signature (DomainKeys)
- Publish public-key in DNS
  Sign mail with private-key
- Receiver verifies signature
- Original Sender is authenticated
- In transit modifications may invalidate signature
- Senders have to deploy a software change
- Easy on forwarders
- Verifies mail contents
- Can be extended to per user authentication (encryption?)

- Digital signatures is the best long term scheme but you can
  - Use SPF and SIDF now!
  - Multiple schemes are better than one.

So why should I worry about evolving standards?

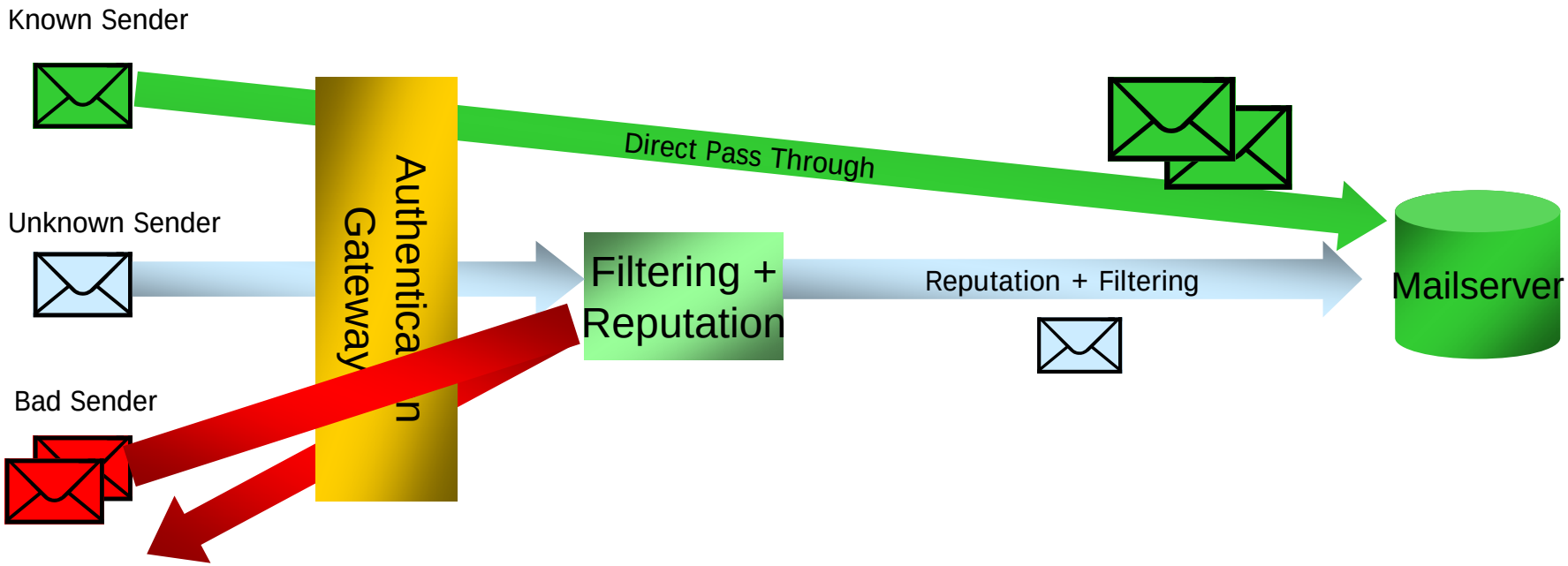
SENDMAIL®

"From October, AOL, Yahoo, Hotmail, Earthlink and Comcast want those that send lots of messages to their users to comply with new mail standards.

The five big firms want every organisation that sends out lots of e-mail, including spammers, to comply with technical standards known as the Sender Policy Framework (SPF) and Sender-ID."

Source: BBC News 1 October 2004

The Future....



- Put the user in control
  - Allow wanted messages and stop unwanted messages
- Today – Filter out bad stuff based on
  - Bad Content Characteristics – Always changing: new spam domains, content techniques etc
- Future – Filter in good stuff based on
  - Sender, Reputation, Accreditation – very stable data

Sendmail Testing

SENDMAIL.NET

SENDMAIL®

- Gauge attributes of each scheme
  - Survivability
  - End-user Experience
  - Deployability
  - Performance
  - Security
- Present results and recommendations for different users
- Open source milters available now at:

sendmail.net

Status and Next Steps

SENDMAIL®

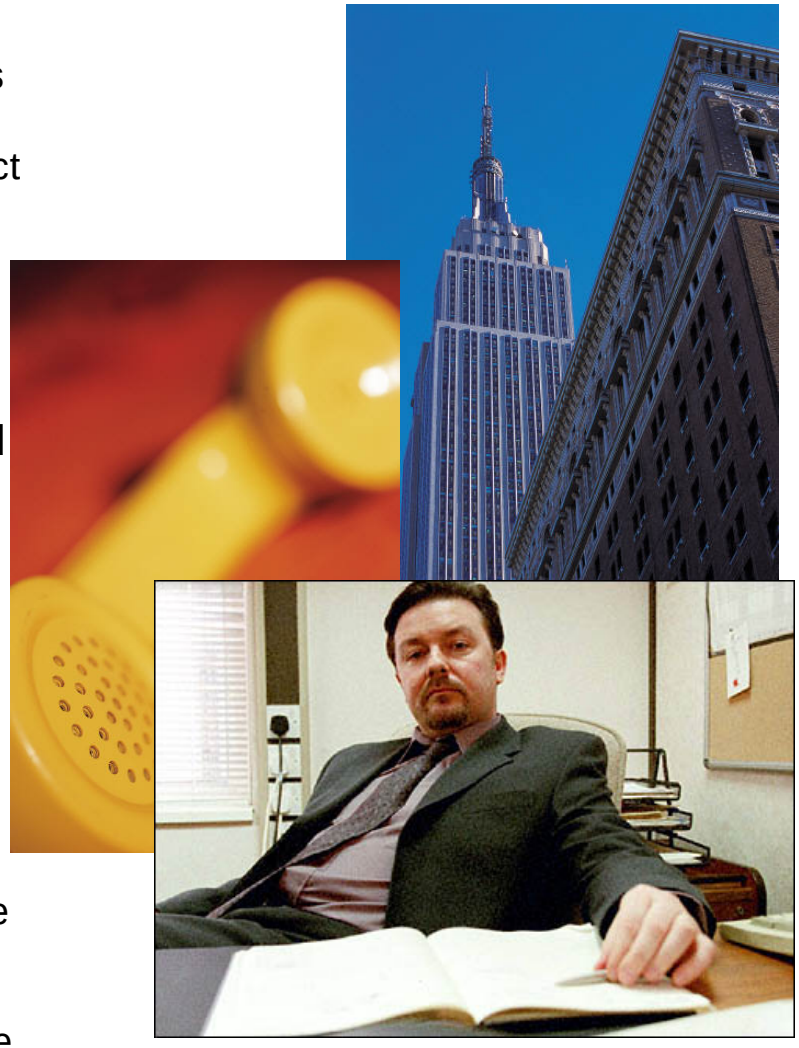
- SIDF
- IETF has tabled SIDF due to patent issues
  - Sendmail's perspective on this issue

- DomainKeys
- Internet draft submitted May 17 to IETF
- Working with IETF to determine next steps
- A few other approaches – some being combined
  - Sendmail has published plug-ins for testing
  - Yahoo! released a royalty free reference implementation for DomainKeys
  - Qmail patch in private trial
  - Yahoo.com plans to trial later this year

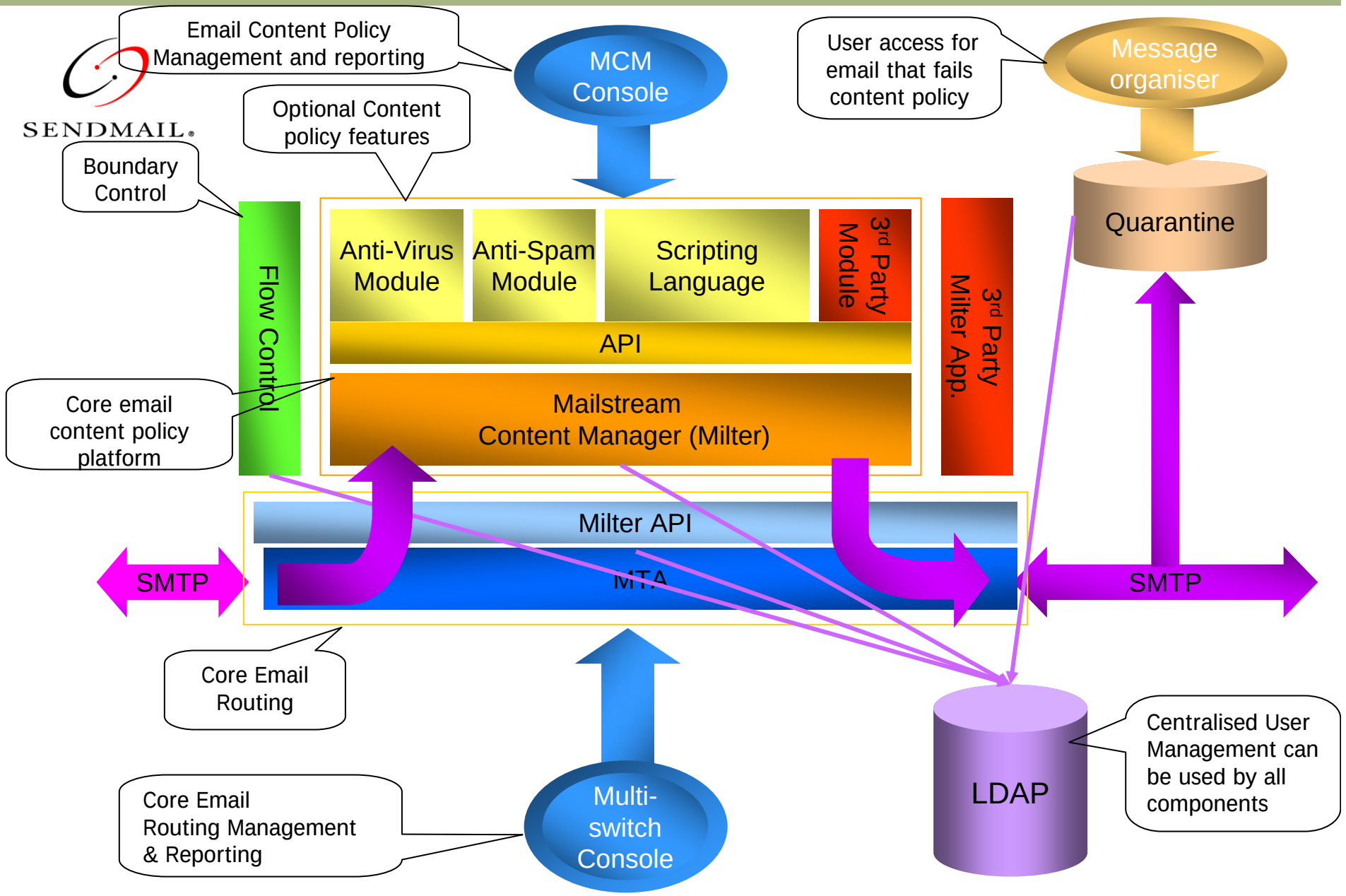
Beyond SPAM: Internal Collaboration and Compliance

SENDMAIL®

- Collaboration
  - Email service is a critical tool for internal and external communications
    - Service Level Agreements
  - Its 2nd to the telephone and we expect 99.9% availability from telephony services
  - Application driven Email part of Business Process Automation
- Business Policies need to be reflected by Email system
  - **Legal:** Regulatory Legal: Regulatory Monitoring
    - Global
      - Sarbanes Oxley
      - Basel II
    - UK or EU
      - Data Protection act
      - Freedom of Information act (UK)
  - **Operational:** Commercially Sensitive Material
  - **HR:** Abuse / Inappropriate use of email system by employees e.g. claire swire email that went global

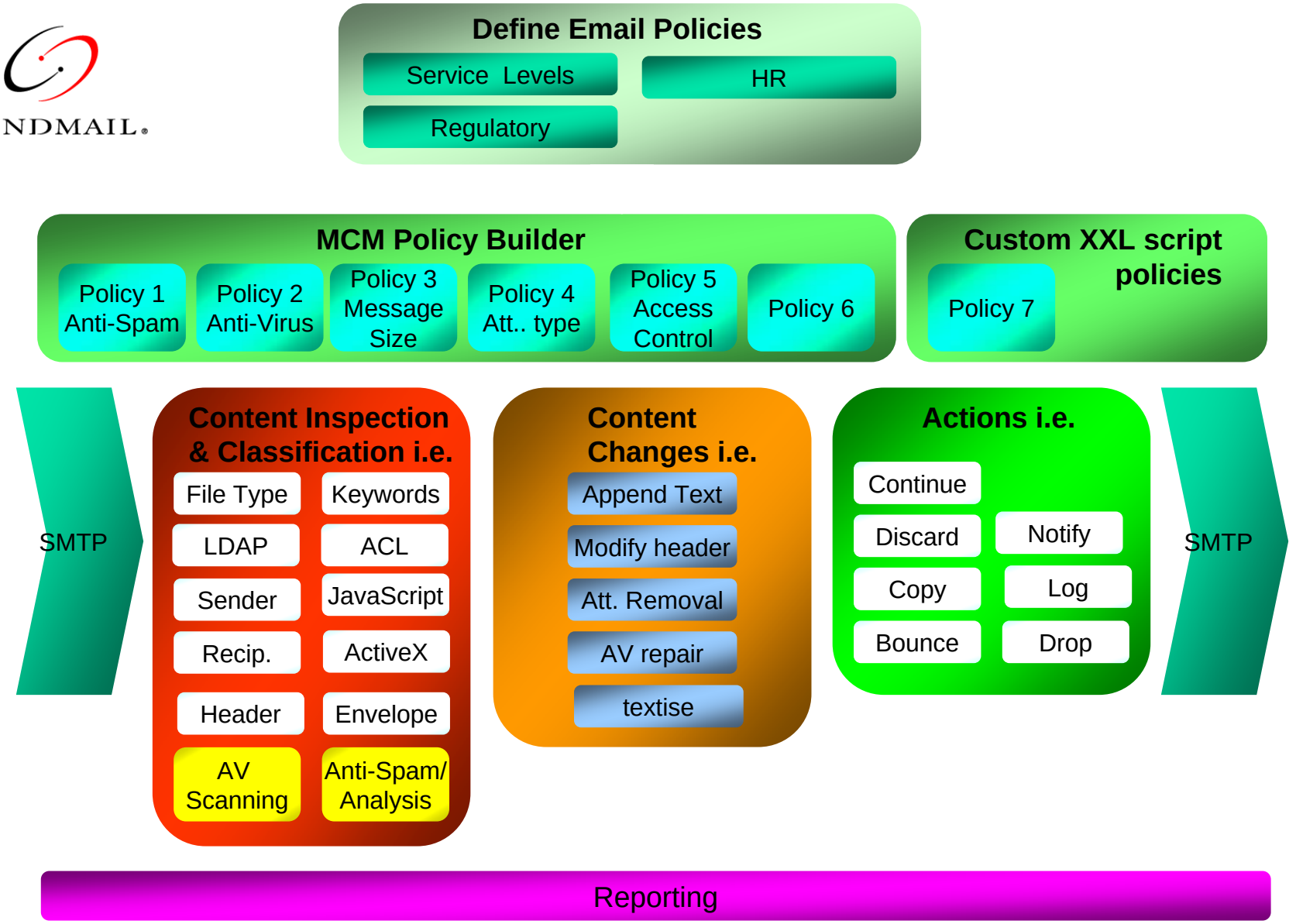


Sendmail Solution – Platform Overview

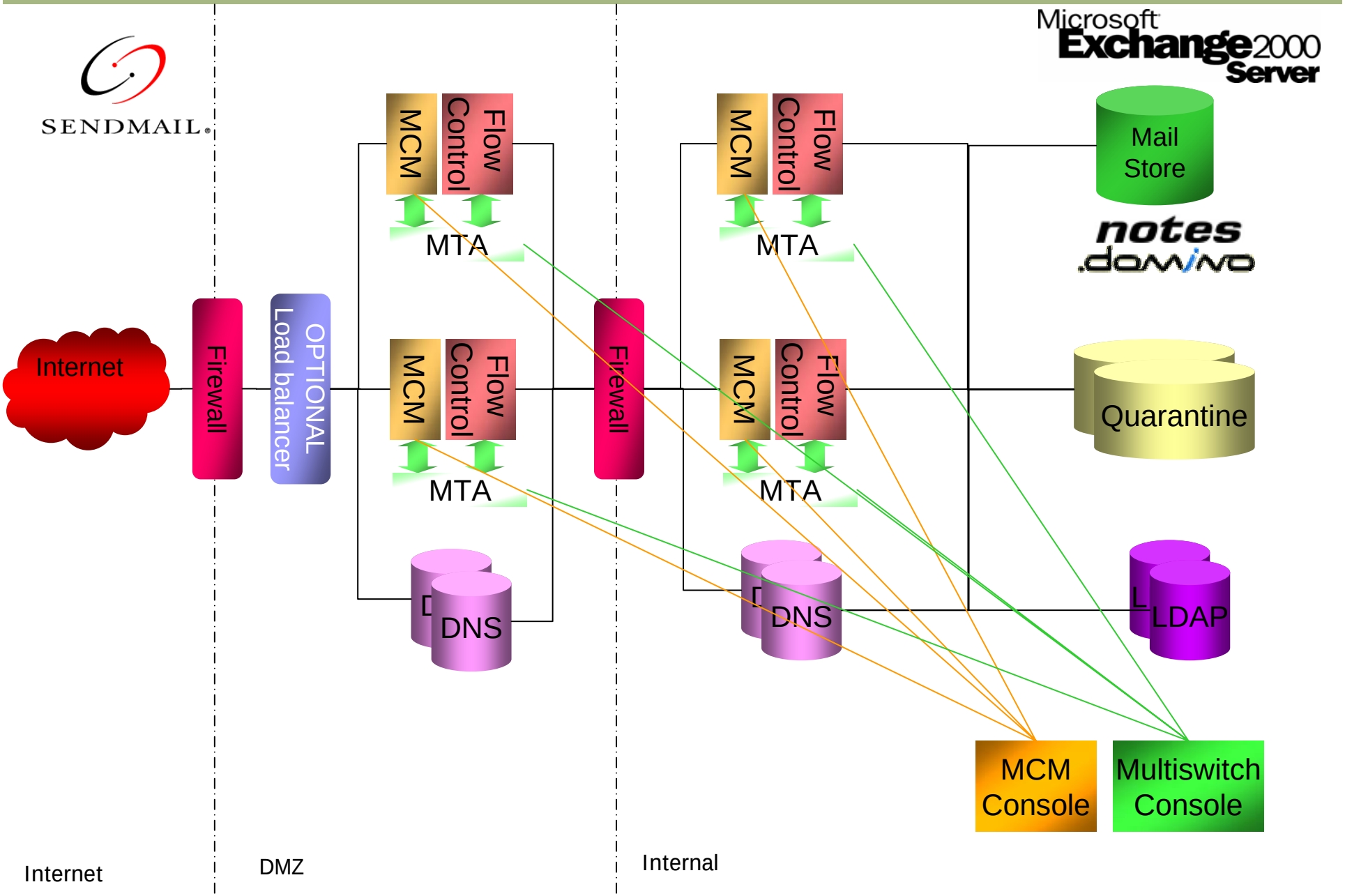


Complete Email Content Policy management

SENDMAIL®



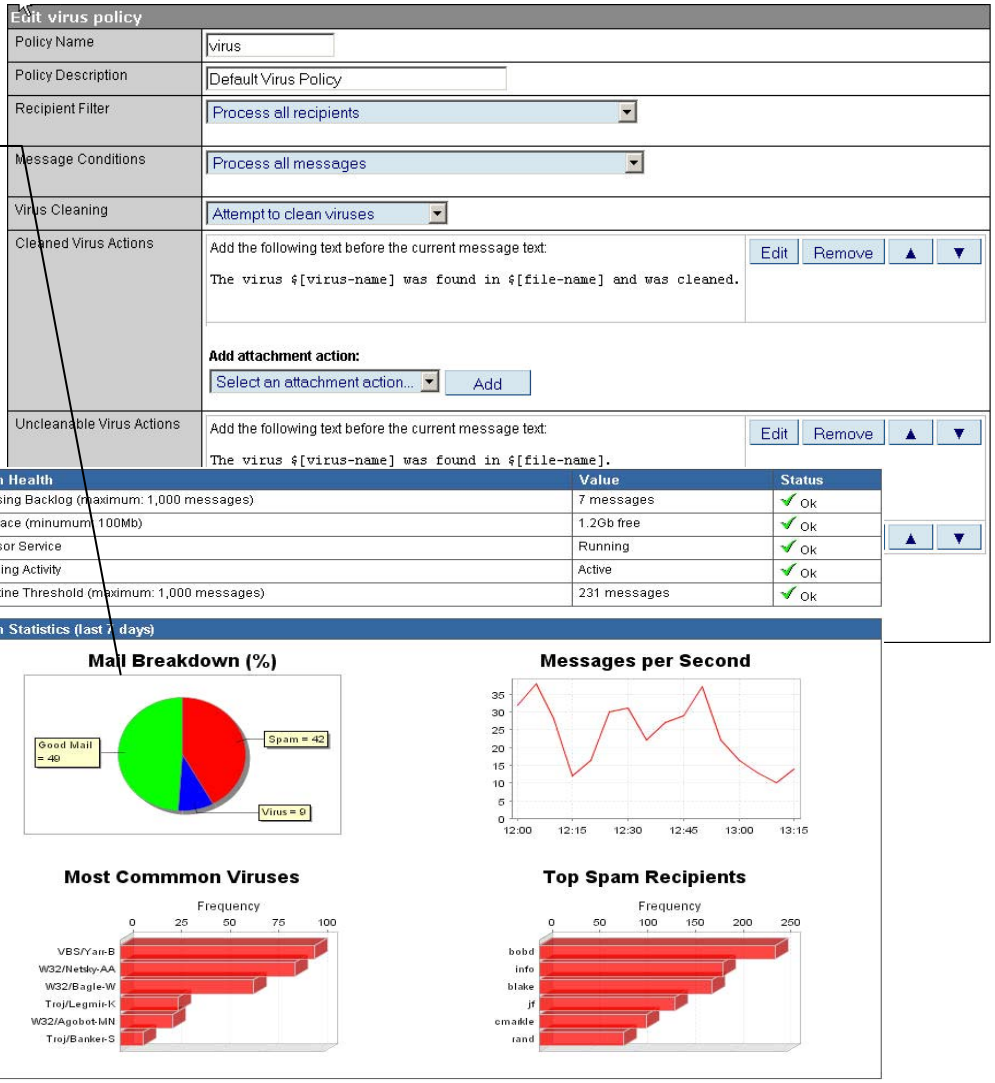
Distributed Architecture – 24 x 7 availability



Centralized Management and Reporting - MCM

SENDMAIL®

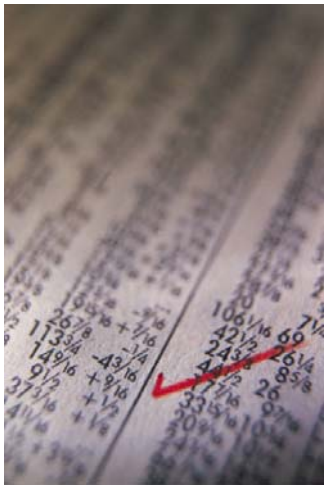
MCM standard reports include
- Number of spam messages detected
- Overall spam message percentage
- Top Spam recipients.
- Top Viruses encountered
- Number of messages processed
- Number of policies executed
- Graphical sort of number of messages per policy



Email Management Best Practices Checklist

SENDMAIL®

- Do not accept Internet email that's not for you
  - Make sure any email received is only for valid users
    - LDAP for routing / boundary control ✓
- Control email content at the Internet Gateway
  - Manage email content
    - Identify SPAM ✓
    - Identify Viruses ✓
    - Enforce email compliance (regulatory) ✓
    - Sender Authentication (Future)
- Management and Reporting
  - Do you have policies for: ✓
    - Security ✓
    - Compliance ✓
    - Service Level
  - Centralized management and administration



How do you score??

SENDMAIL®

Summary

SENDMAIL®

- Key challenge is centralized defence management of increasing volumes and security threats via email
- Sender Authentication will “filter-in” good mail as opposed to “filter out” bad mail
- SPAM is a headline issue today, the real issue that should concern enterprises is Phishing (email fraud) and the damage it can do their brand as well as customers
- Email Compliance is the next challenge in several sectors soon i.e. Finance, Healthcare, Pharmaceuticals