



SPAM prevention & elimination for Domino Server

Presented By: **Frank Docherty**

The aim of this session is:

To help you **manage** and **reduce** the volume of email SPAM that you receive:-

- by securing your Domino Server SMTP configuration
- by utilising **only** the tools that are available within Lotus Domino Server

Disclaimer

Lotus Domino has no built in AV scanning capabilities

I can show you how to configure Lotus Domino server to scan for emails with potential viral payloads (exe, com, vbs, etc.), but I cannot show you how to turn your Domino Server in to an Anti Virus scanning engine, without the assistance of third party software products.

- **Introduction**
- **Why should I use Domino for my SMTP security?**
- **Securing your SMTP Configuration**
- **Blacklists & Whitelists**
- **Server Mail Rules**
- **Quarantine Management**
- **Q&A**



Why should I use Domino for my SMTP security?

I already have an SMTP security solution – Why should I use Domino Server?

Domino SMTP security features are built in, and don't require any third party add-ons

Domino Server can compliment your existing SMTP security solution, by providing a secondary layer of protection

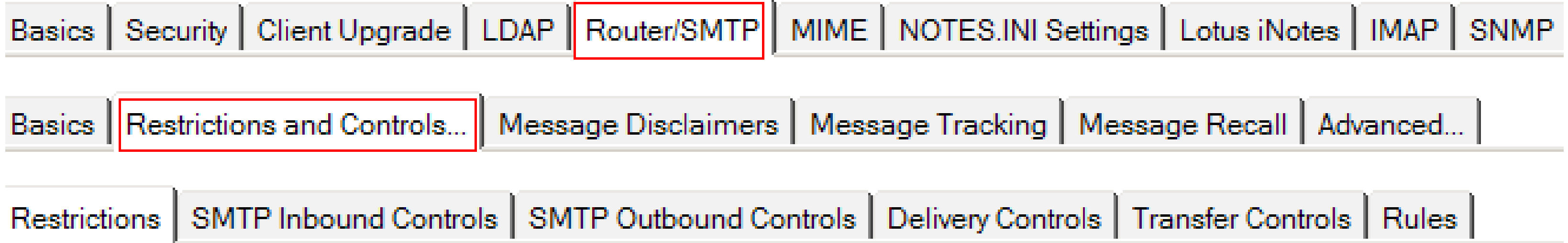
You can use the native SMTP security features of Domino server within development, test & pre-production environments

Security of your SMTP configuration is already built in, thanks to the Domino Server security model

This can save you a **lot** of money on licensing costs for 3rd party SMTP security products



Securing your Domino Server's SMTP configuration will prevent potential email Spammers from exploiting your server's SMTP delivery capabilities.



SMTP Security configuration settings are contained within a Domino Server Configuration Settings document. These settings can be found under the Router/SMTP, Restrictions and controls tab of the server configuration settings document.

The following slides will focus on securing your configuration settings within the Restrictions, SMTP Inbound & SMTP Outbound controls tabs.

Applying restrictions to the SMTP Router task

The fields within the Restrictions tab control **Domino Server** restrictions that can be applied to the SMTP router task.

Router Restrictions

Allow mail only from domains: ACME
NDGUY
DACS

Deny mail from domains: EXCHANGE
OUTLOOK

Allow mail only from the following organizations and organizational units: (* /Acme, * /Sales/Corp)

Deny mail only from the following organizations and organizational units: (* /Acme, * /Sales/Corp)

Maximum message size: 2048 KB

Send all messages as low priority if the message size is between: Enabled
1560 KB and the maximum message size.

Prevent your Domino server from becoming an Open Relay

It is **very important** that you secure your server's SMTP configuration, in order to prevent yourself from becoming an Open Relay.

Inbound Relay Controls

Allow messages to be sent only to the following external internet domains:

Deny messages to be sent to the following external internet domains: (* means all)

Allow messages only from the following internet hosts to be sent to external internet domains:

ndguy.co.uk
loveablegeek.co.uk

Deny messages from the following internet hosts to be sent to external internet domains:(* means all)

ihatenotes.com
notessucks.com

Inbound Relay Enforcement

Perform Anti-Relay enforcement for these connecting hosts:

All connecting hosts

Exclude these connecting hosts from anti-relay checks:

192.168.*.254

Exceptions for authenticated users:

Perform anti-relay checks for authenticated users

Restrict SMTP Hosts from connecting to your server

If you have other servers and/or client PCs that have the ability to send SMTP email, then you can control which SMTP hosts are allowed to connect to your Domino Server.

Inbound Connection Controls

Verify connecting hostname in DNS: Enabled

Allow connections only from the following SMTP internet hostnames/IP addresses: [192.168.0.10]
[192.168.0.20]
notesiscool.com

Deny connections from the following SMTP internet hostnames/IP addresses: [192.168.254.200]
[192.168.254.210]
notessucks.com

Error limit before connection is terminated:

Restrict users from sending SMTP mail

You can also limit which users can send SMTP email via your server

Outbound Sender Controls

Allow messages only from the following Internet addresses to be sent to the Internet:

Deny messages from the following Internet addresses to be sent to the Internet: #Sin_Bin_SMTP_External

Allow messages only from the following Notes addresses to be sent to the Internet:

Deny messages from the following Notes addresses to be sent to the Internet: #Sin_Bin_SMTP_Internal

Other Considerations for Securing Your SMTP Configuration

Is port 25 secured within your local area network?

Do all of your Domino Servers **really** need to run the SMTP listener task?

Where are your Domino SMTP servers placed within your network infrastructure?

If you get your SMTP traffic from a single address (e.g., your ISP), is that connection secured?

Should consider securing your SMTP traffic by utilising TLS?

Summary

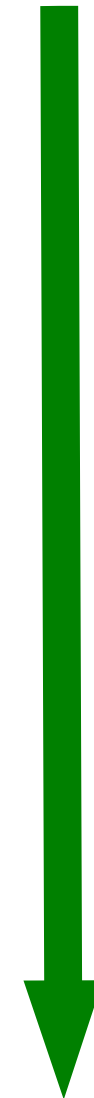
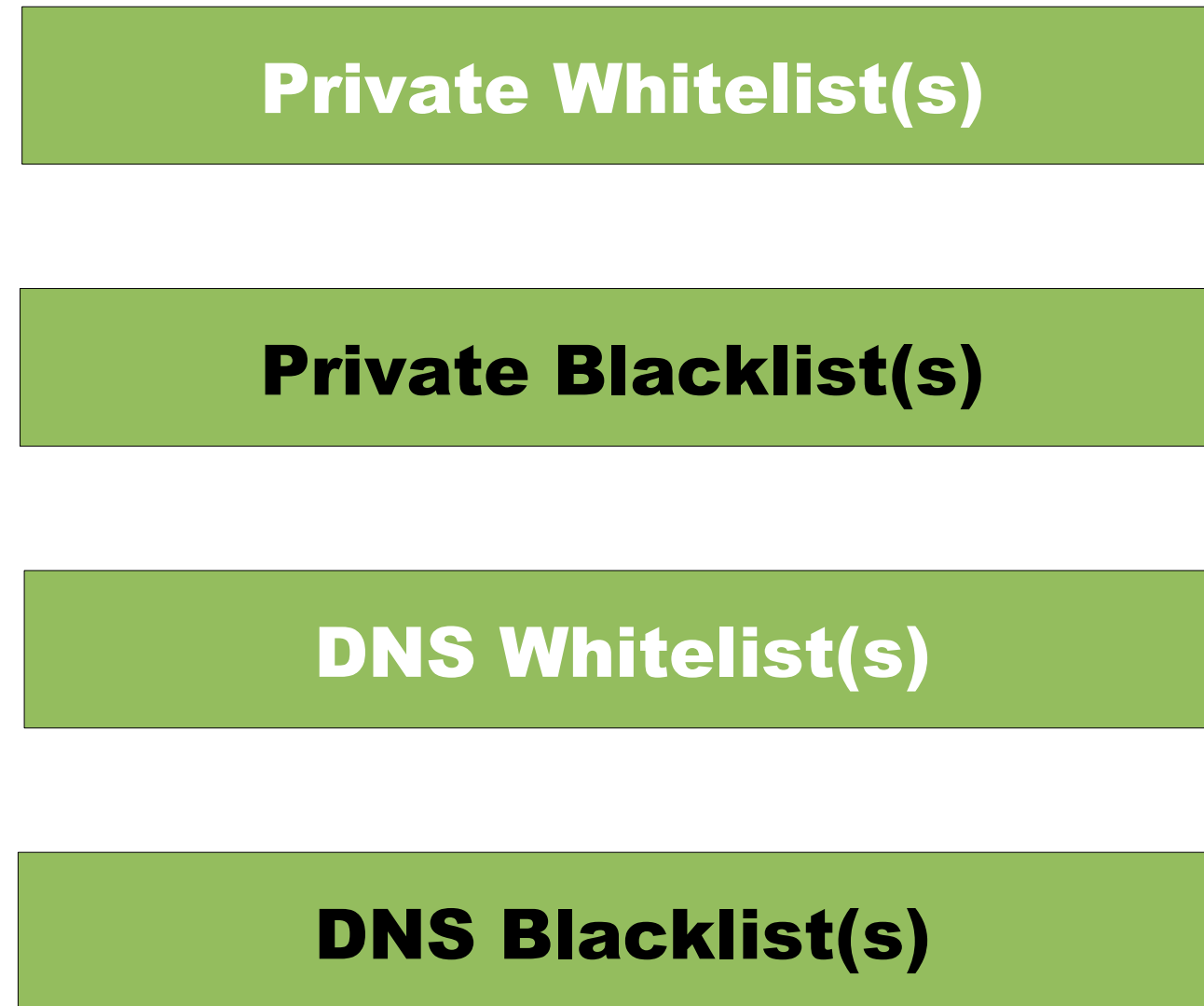
- Apply Domino domain level routing restrictions to the Domino Server SMTP Router via the Router Restrictions section within the Restrictions Tab
- Prevent your server from becoming an open relay by updating the Inbound Relay Controls and Inbound Relay Enforcement sections within the SMTP Inbound Controls Tab
- Control which devices can & cannot connect to your Domino server by entering them within the Inbound Connection Controls section located on the SMTP Inbound Controls Tab
- Limit which users can & cannot send SMTP traffic from your Domino server by entering them within the Outbound Sender Controls section located on the SMTP Outbound Controls Tab



**“It’s not the most sophisticated Spam blocker
I’ve tried, but it’s the only one that works!”**

By utilising public & private DNS lists within your Domino Server SMTP configuration, you can control which hosts you want to accept SMTP traffic from.

Order of processing



DNS filter lists are configured from within the SMTP Inbound Controls tab of your server configuration settings document.

Private Whitelist

Private Whitelist Filter

Private Whitelist Filter:	Enabled
Whitelist the following hosts:	#WL_SMTP_Hosts
Desired action when a connecting host is found in the private whitelist:	Log and tag message

You can use private whitelist filters to specify hosts and/or domains to be **excluded** from blacklist checking

Private Whitelist filter actions

Action	Explanation
Silently skip blacklist filters	No logging occurs and all blacklist filters are skipped
Log only	Logs the host name and IP address of the connecting host found within the private whitelist
Log and tag the message	As above, but also adds "PrivateWhitelist" to the \$DNSWLSite field of the message

Hosts that are specified within private whitelists are exempt from blacklist checks, but still subject to relay enforcement checking

Whitelists can be used independently of blacklists

If a connecting host is found on your private whitelist, **all** other private blacklist, DNS whitelist, and DNS blacklist checks are **skipped**.

Use Private DNS Whitelists with caution – be 100% certain of the hosts that you whitelist

Private Blacklist

Private Blacklist Filter

Private Blacklist Filter: Enabled

Blacklist the following hosts: #BL_SMTTP_Hosts

Desired action when a connecting host is found in the private blacklist: Log and tag message

Custom SMTP error response for rejected messages: Sorry. We don't accept mail from %s

Use private blacklist filters to block known spam email domains & hosts

Private Blacklist filter actions

Action	Explanation
Log Only	Records the host name and IP address of the connecting server found in the private blacklist
Log and tag message	Follows the actions of “Log Only”, but also adds “PrivateBlacklist” to the \$DNSBLSite field of the message
Log and reject message	Follows the actions of “Log Only”, and sends a message back to the host telling them that the message has been rejected.

When private blacklists are enabled, the SMTP listener task compares the names of hosts that may be subject to relay enforcement against the private blacklist **prior** to performing DNS blacklist queries. **This prevents unnecessary DNS lookups.**

You (the administrator) control the private blacklist, and it is stored within the Domino Directory, making it easily maintainable

If the host is not found in the private blacklists, processing continues with DNS whitelist filters and then DNS blacklist filters

DNS Whitelist

DNS Whitelist Filters

DNS Whitelist Filters: Enabled

DNS Whitelist Sites: wl.nszones.com

Desired action when a connecting host is found in a DNS whitelist: Log and tag message

Use DNS whitelist filters to allow SMTP email from **non** spamming (i.e., legitimate) email domains & hosts

DNS Whitelist filtering actions

Action	Explanation
Silently skip blacklist filters	No logging occurs and all blacklist filters are skipped
Log only	Logs the host name and IP address of the connecting host found within the private whitelist, as well as the name of the site where the server was listed
Log and tag the message	As above, but also adds the host name of the DNS Whitelist where the message was whitelisted to the \$DNSWLSite field of the message

DNS whitelists can be used independently of blacklists

Private blacklists override DNS whitelists

DNS whitelist filtering applies **only** to hosts subject to inbound relay enforcement.

If a connecting host is found on a DNS whitelist, then all other the blacklist checks are skipped.

DNS Blacklist(s)

DNS Blacklist Filters

DNS Blacklist filters:	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
DNS Blacklist sites:	<input checked="" type="checkbox"/> zen.spamhaus.org
Desired action when a connecting host is found in a DNS Blacklist:	<input checked="" type="checkbox"/> Log and reject message
Custom SMTP error response for rejected messages:	<input checked="" type="checkbox"/> Your host %s was found to be on the %s DNS blacklist - go away, we don't like SPAM here!

Use DNS blacklist filters to block SMTP email from **known** spamming email domains & hosts

DNS Blacklist Filters actions

Action	Explanation
Log Only	Accepts the message, records the host name and IP address of the connecting host (as found in the DNS blacklist), and the name of the DNS blacklist site where the connecting host was found.
Log and tag message	Follows the actions of “Log Only”, and also adds the DNS Blacklist site address to the \$DNSBLSite field of the message
Log and reject message	Follows the actions of “Log Only”, and sends a message back to the host telling them that the message has been rejected. This message is customisable by the administrator

Domino performs DNS blacklist checks **only** on hosts that are subject to relay enforcement checks.

Any host that is authorised to relay through your Domino Server is **exempt** from blacklist checks. **This prevents unnecessary DNS lookups.**

If the connecting host is found in the DNS blacklist, all other the blacklist checks are skipped.

General Considerations when using filter lists

If you use public DNS blacklist or whitelist filtering listings, **ensure** that your Domino Server can query your chosen DNSBL/WL listing sites.

Limit the number of external DNS Blacklist and Whitelist services you use for filtering, as each message you receive will be compared against these listings

If you normally receive high volumes of SMTP traffic, and really, really, really need to compare every message against multiple DNS Black & White listings, consider caching these listings locally, and synchronising them regularly

Choose your filter actions carefully. Some DNS listings are more prohibitive than others, and may generate higher amounts of false positives (i.e., - cause you to lose messages) if you only log & reject

Review your public filter list choices on a frequent basis. Are they being regularly updated? Are they still providing you with effective protection?

Likewise, ensure that you maintain your own private black & white listings, to ensure that you are adequately protected.

Summary

Private Whitelists → Private Blacklists → DNS Whitelists → DNS Blacklists

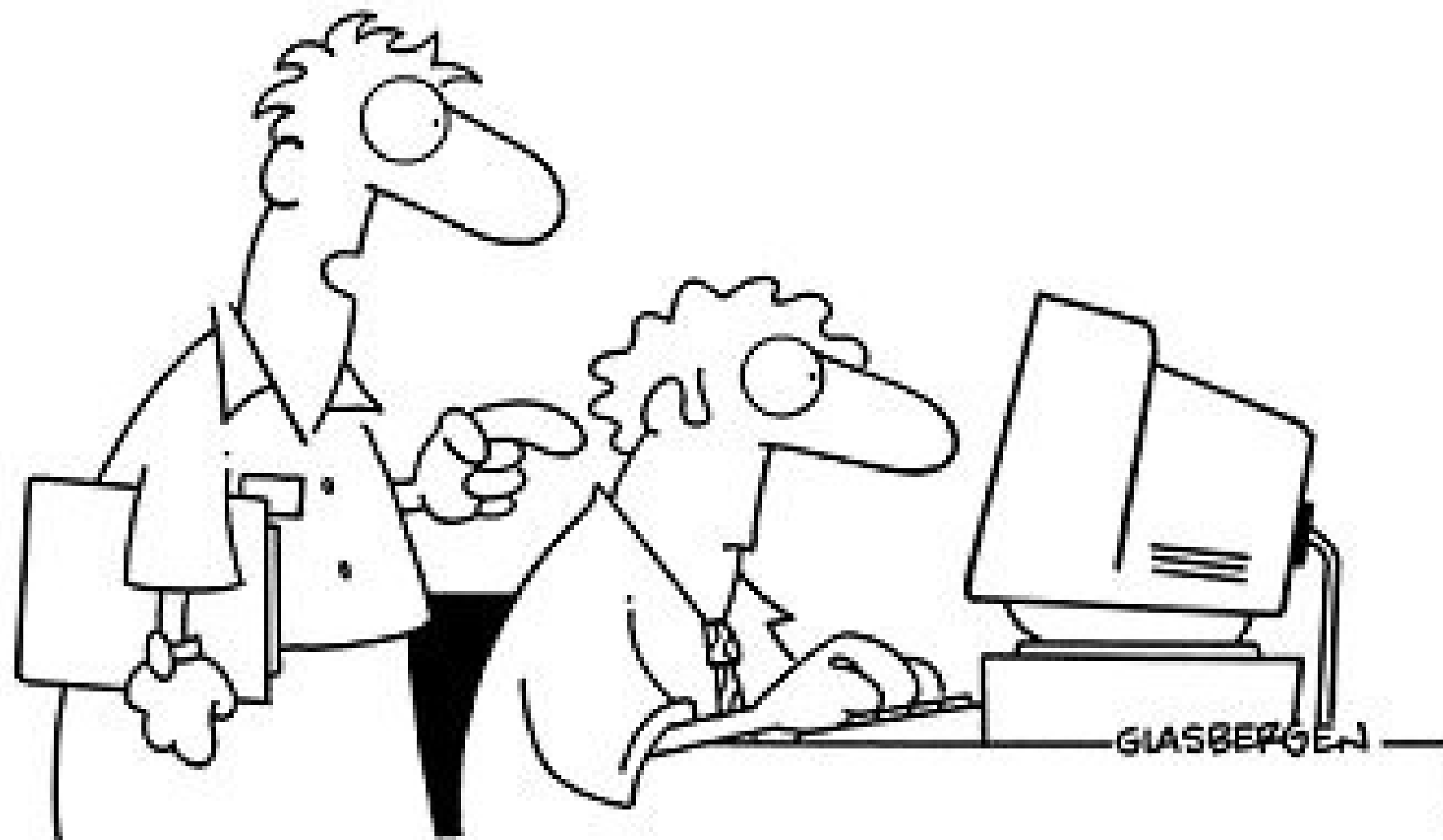
Private lists are maintained by **you**, and stored within **your** Domino Directory

All listing types give you multiple filtering options, with “Log & tag message” being common to all of them. This is very useful when used in conjunction with Server Mail Rules

DNS blacklist & whitelist filtering applies **only** to hosts subject to inbound relay enforcement. This reduces the need for DNS lookups, and helps to maintain performance levels








DNS whitelists can be used independently of blacklists but private blacklists override DNS whitelists

Be 100% certain of **any** host that you whitelist



**“We found a solution to your spam problem.
We replaced all of the keys with ‘delete’ buttons.”**

Server mail rules can assist you in your fight against email SPAM, by taking the appropriate action(s) against filtered email.

 New Rule...  Edit Rule...  Delete Rule  Move Up  Move Down  Enable Rule  Disable Rule

- ✓ When Form is Memo AND Sender does not contain Power Users/ndguy AND Attachment names contains EXE change Routing State - mark as Held
- ✓ When Form is Memo AND Sender does not contain /Power Users/ndguy AND Attachment names contains M4R change Routing State - mark as Held
- ✓ When Attachment names contains EXE AND Attachment names contains VBS AND Attachment names contains CMD AND Attachment names contains BAT AND Attachment names contains COM AND Attachment names contains MP3 AND
- ✓ When All Documents AND BlackList tag contains PrivateBlacklist change Routing State - mark as Held AND Stop Processing further Rules
- ✓ When All Documents AND BlackList tag contains bl.nszones.com change Routing State - mark as Held AND Stop Processing further Rules
- ✓ When Size is less than 900 bytes(s) AND Recipient Count is greater than 50 change Routing State - mark as Held AND Stop Processing further Rules
- ✓ When All Documents Journal this Message

Server mail rules allow you to create content filtering rules that define the actions to take on all or certain messages

At startup, the server retrieves the defined server mail rules from the Server Configuration Settings document and registers them as monitors on each MAIL.BOX database in use

Filter Criteria

Sender
Subject
Body
Importance
Delivery priority
To
CC
BCC
To or CC
Body or subject
Internet domain
Size (in bytes)
All documents
Attachment name
Number of attachments
Form →
Recipient count
Any recipient
Blacklist tag
Whitelist tag

Logical Operators

contains (for text field values)
does not contain (for text field values)
is
is not
is less than (for numeric field values)
is greater than (for numeric field values)

Form Types

Appointment
Delivery Report
Memo
Non Delivery Report
Notice
Reply
Return Receipt
Trace Report

Filter Actions

Journal this message
Move to database
Don't accept message
Don't deliver message
Change routing state
Stop processing

Server Mail Rule Filter Actions

Action	Explanation
Journal this message	The Router sends a copy of the message to the configured Mail journalling database and continues routing the message to its destination
Move to database	The Router removes the message from MAIL.BOX and moves it to a database of your choice, and the message is not routed to its destination
Don't accept message	<p>The message is rejected, but the Router does not generate a delivery failure report. Depending on the message source, the sender may or may not receive an NDR or other indication that the message was not sent.</p> <ul style="list-style-type: none">– If the message is routed over SMTP, then an SMTP 500 error is generated and sent– If the message is routed via Notes routing, then a delivery failure report is generated and sent– If the message is deposited via Notes, then the sending client displays an error indicating that the message violated a mail rule.
Don't deliver message	<p>The message is accepted, but rather than sending it to its destination, it processes the message according to one of the following options:</p> <p>Silently delete - the message is deleted from MAIL.BOX with no indication to the sender or recipient Send NDR - an NDR is generated and returns it to the sender.</p>
Change routing state	The message is accepted, but it is not delivered. Instead, the message is marked as held by changing the value of the RoutingState field on the message to HOLD . The message remains in MAIL.BOX until it is released by the administrator.
Stop processing	Domino stops processing any further rules that apply to the message

Considerations when using server mail rules

Rules are processed in the order in which they are displayed

Try and limit the number of rules that you use

Each message is evaluated only once - be aware of where you stop rule processing

You can't use server mail rules to perform virus scans of inbound messages, but you can use them to quarantine known executable file types, or any other potentially malicious file types

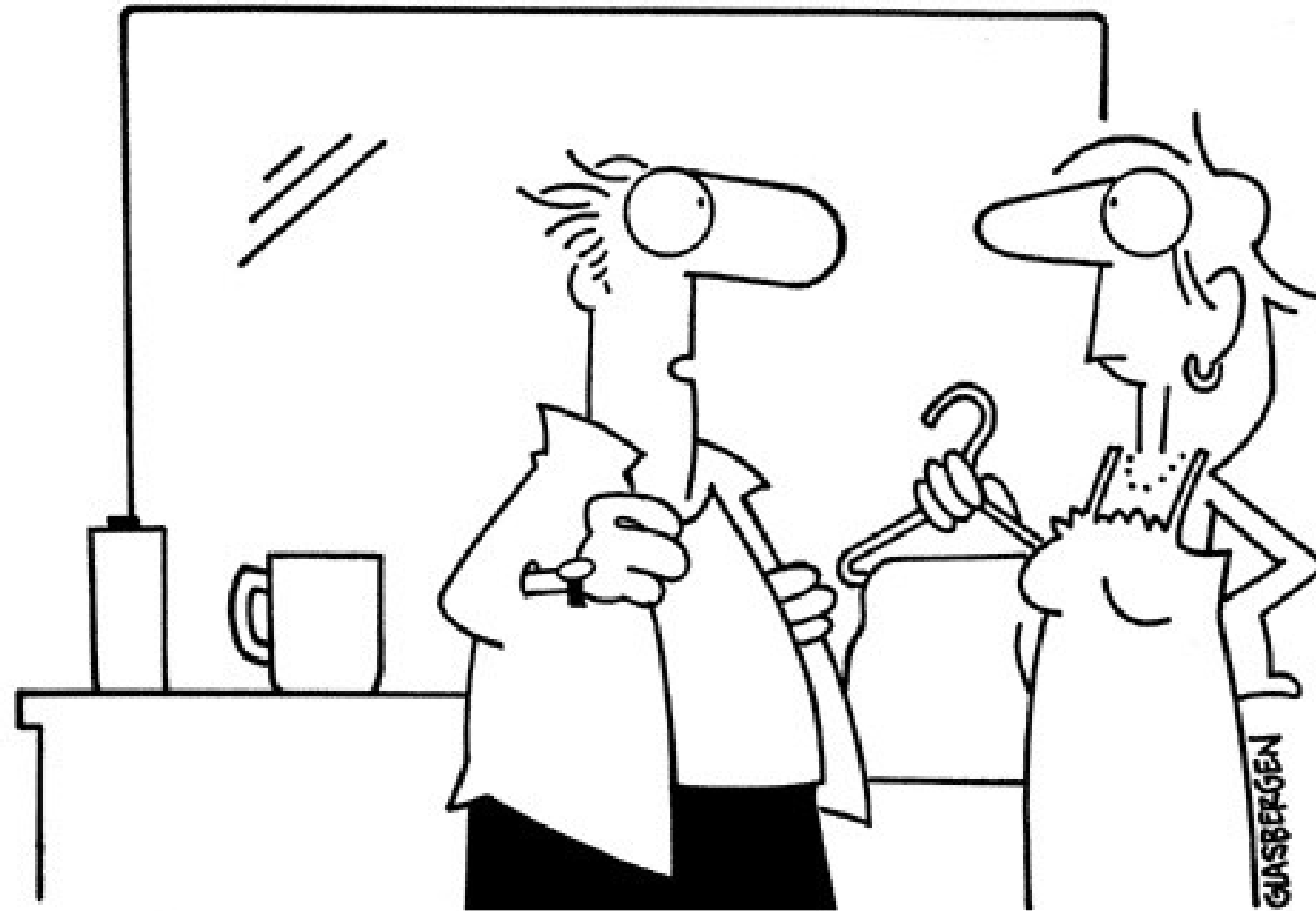
If you use the “move to database” action within your rules, be sure that you have created the appropriate quarantine database(s) **before** enabling your rule(s)

When you add or update a rule within your configuration settings document it will be enabled immediately

Always, always, always, always, always, always, **ALWAYS** take a backup of your server configuration settings document **BEFORE** you add/update server mail rules.

Summary

- Create server mail rules to filter, quarantine & reject messages
- Create & update server mail rules within your Server Configuration Settings document
- Server mail rules are registered as monitors on each MAIL.BOX at server startup
- The server evaluates the fields contained within the message against the registered mail rules
- Server mail rules are processed in the order they are stored within the server configuration settings document
- Each message is evaluated only once



"I get to the office around 8:45, pour myself a cup of coffee, turn on my computer, delete all the spam, and then it's time to go home."

By trapping, or quarantining, certain types of messages, you help **reduce** the risk of delivering malware infected messages to your user mailboxes.

Held Messages

- Let common sense prevail! Don't release **any** held messages until you are 100% certain that they are legitimate
- To determine the legitimacy of a message, check the mail routing events view within your log file. If you are logging & tagging messages, you will see what has been trapped, and where it was flagged as SPAM (i.e., on a private blacklist or public DNS blacklist site)
- Messages marked as held are stored in your server's MAIL.BOX files. Be sure to check ALL of the MAIL.BOX files on each of your servers, especially if you are using multiple MAIL.BOX files

Releasing Held Messages

Use the message release options within the MAIL.BOX database to release messages to their intended recipients:-

Release... ▾		Delete Message		
Submit Time	From ^	Recipients ^	Size (Kb)	Failure Reason
! 05/11 18:35	FDocherty@Worldmark.com	sys.admin@ndguy.co.uk	6.2	
! 05/11 19:38	Frank <frank.docherty@gmail.com>	sys.admin@ndguy.co.uk	3.7	
! 05/11 19:47	Frank <frank.docherty@gmail.com>	sys.admin@ndguy.co.uk	3.8	
! 08/11 20:12	Test User/Power Users/ndguy	frank.docherty@gmail.com	655.1	
! 08/11 20:15	Test User/Power Users/ndguy	fdocherty@worldmark.com	654.8	
! 08/11 20:21	Sys Admin/ndguy	<FDocherty@Worldmark.com>	655.0	
! 08/11 20:39	Sys Admin/ndguy	<FDocherty@Worldmark.com>	357.7	
! 08/11 20:41	Test User/Power Users/ndguy	frank.docherty@gmail.com	357.6	
! 08/11 20:52	Sys Admin/ndguy	<FDocherty@Worldmark.com>	429.7	

Quarantined Messages

- Again - Don't release **any** quarantined messages until you are 100% certain that they are legitimate and don't contain any malware
- Quarantined messages will typically be messages which have one or more known attachment types, which you block within your configuration
- Store these in a database created from a mail template or from a mailbox router template. This will make it easier to manage and, if necessary, release the messages from quarantine.

Summary

- Be sensible about what held & quarantined messages you choose to release
- Don't succumb to user pressure to release ANY email until you check it first, and are 100% certain the message is legitimate
- Check your MAIL.BOX files and quarantine databases on a regular basis

- Secure your Domino Server SMTP Configuration in order to ensure that you are not an Open Relay
- Restrict which Domino Domains & internal SMTP hosts connect and relay through your Domino server
- Limit which users can and cannot send SMTP mail
- Control which external hosts can connect to your Domino SMTP server by utilising private & public DNS lists
- Filter messages, based on broad range of criteria, by employing Server Mail Rules
- Hold or quarantine messages you are not 100% certain about
- Regularly check your held and quarantined items

Thank you for attending

Please remember to complete your session evaluation form.

Blog: <http://www.theloveablegeek.co.uk>

Email : loveable.geek@gmail.com