
maps

Application Note:

**How to secure your mail system
against third-party relay**

Here are some pointers on how to secure your current mail system against third-party relay. Locate your mailer in the table below, and jump to the suggestions on what to do.

Altavista Mail for Windows-NT 2.0	1
Appleshare IP Server (ASIP).....	1
Artisoft XtraMail.....	1
AS/400 TCP/IP Connectivity Utilities/400	1
CommuniGate	2
DataEnter SMTPBeamer	2
DIGITAL TCP/IP Services for OpenVMS.....	2
DMail.....	2
EMWAC IMS.....	2
Eudora Internet Mail Server (EIMS).....	3
Eudora WorldMail Server.....	4
exim	4
FloosieTek FTGate.....	4
Gauntlet.....	4
Groupwise	5
IMail Server.....	6
InterMail.....	6
International Messaging Associates Internet Exchange	6
Isode Message Switch	7
IT House Mail Server.....	7
Lotus cc:Mail	8
Lotus Notes and Lotus Domino (up to R5).....	8
Lotus Domino R5 and above.....	9

LSMTP	10
Lyris.....	10
MailSite	10
Mailtraq.....	11
MDaemon.....	11
Mercury.....	11
Message Exchange (MX).....	12
Messageware MTA.....	12
Microsoft Exchange Server.....	13
M MDF.....	13
Multinet for OpenVMS.....	13
Netscape Messaging Server	14
NTMail.....	14
Obtuse smtpd	16
pmdf	16
Postfix.....	17
Post.Office	17
Qmail	17
QuickMail Pro Mac 1.1.1r1 Server.....	18
QuickMail Pro Windows (95/NT) 1.5 Server.....	18
rblsmtpd	19
Seattle Lab SLMAIL	19
Sendmail Version 5.....	20
Sendmail Version 8.....	20
Sendmail Pro	21
Smail.....	21
SmartMax MailMax.....	22
Stalker Internet Mail Server (SIMS).....	22

Sun Internet Mail Server	22
Symantec Norton Anti-Virus for Gateways	22
TFS Gateway.....	23
TIS FireWall ToolKit (FWTK) smap/smapd	23
Vircom VOPmail.....	23
VM/CMS	24
VM/ESA TCP/IP	24
VM SMTP	24
ZMailer.....	24



Altavista Mail for Windows-NT 2.0

Status: **OBSOLETE**
Systems: Windows/NT
INFO: <http://www.altavista.software.digital.com>

To disable relaying you will need a software update, which used to be available from Compaq. However, now that Compaq has retired the entire AltaVista Mail product line, there may be no option left but to change to a modern product.

Appleshare IP Server (ASIP)

Status: Commercial
Systems: Mac
Info: <http://www.info.apple.com/kbnum/n31108>

Information on how to secure the Appleshare IP Server against mail relaying can be found at the above link.

Artisoft XtraMail

Status: Commercial ([Artisoft](#))
Systems: Windows
Info: <http://www.artisoft.com/>

XtraMail 1.2 and above support an IPALLOW file, which lets you list which IP addresses will be allowed to relay through your server. Information on this is in Articom Technote TN4077.

AS/400 TCP/IP Connectivity Utilities/400

Status: Commercial ([IBM](#))
Systems: AS/400
Info: <http://www.redbooks.ibm.com/abstracts/gg243442.html>

For OS/400 V4R2 apply PTF SF 53394 (or supercedes). Follow the instructions in the cover letter.

For OS/400 V4R3 apply PTF SF 54553 (or supercedes). Follow the instructions in the cover letter.

For OS/400 V4R4 apply PTF SF 54611 (or supercedes). Follow the instructions in the cover letter.

CommuniGate

Status: Commercial ([Stalker Software](#))
Systems: Mac, NT, Unix, BeOS
Info: <http://www.stalker.com/CommuniGate/>

<http://www.stalker.com/CommuniGatePro/AntiSpam.html#Relay>

DataEnter SMTPBeamer

Status: Commercial ([DataEnter](#))
Systems: Win/NT, Win2000
Info: <http://www.dataenter.co.at/#SMTPBeamer>

SMTPBeamer appears to have fully sufficient relay controls, documented at http://www.dataenter.co.at/doc/smtplibeamer_admin_options.htm#Relay. They also support RBL and DUL queries, but not other lists.

DIGITAL TCP/IP Services for OpenVMS

Status: Commercial
Systems: OpenVMS

The current versions of DIGITAL TCP/IP Services for OpenVMS have relay turned off by default. If it is turned on, it can be disabled by issuing the command:

```
$ucx set config smtp /options=norelay
```

DMail

Status: Commercial
Systems: Windows (NT, 95, 98), Linux (Intel, SPARC, MISP),
FreeBSD, BSD/OS (3 and 4), AIX, Solaris (SPARC, x86)
Info: <http://netwinsite.com>

Instructions on how to disable relaying are in the [online manual](http://netwinsite.com/dmail/manual.htm), <http://netwinsite.com/dmail/manual.htm>.

EMWAC IMS

Status: Freeware
Systems: Windows
Info: <http://ww1.sica.com/IMS/>

The European Microsoft Windows NT Academic Centre (EMWAC) in Scotland has produced IMS (Internet Mail Server), a free Windows/NT mailer. As of the most recent release (version 0.83), it appears that EMWAC IMS has *no* provisions to prevent unauthorized relay.

[SICA Consulting Services](http://www.sica.com/) (<http://www.sica.com/>) has an add-on service that is a possible solution to this problem. First, you need to install SCMSFILTER, a service that that adds filtering capability to IMS. Then, install the antirelay plugin.

Eudora Internet Mail Server (EIMS)

Status: Commercial ([Qualcomm](#))
Systems: Mac
Info: <http://www.eudora.com/eims/>

EIMS version 3 includes more relay control features than previous versions of EIMS. We do not yet know the specifics.

EIMS version 2.0 and above include (possibly inadequate) relay blocking. Here is how to turn it on:

Connect to your server using EIMS Admin.

Open the preferences window by selecting *Preferences* under the *Admin*.

Click on the *Relay Restrictions* icon.

Click the button for *Only route for local domains and the following domains*.

Enter in any domains that should be allowed to relay through your mail server.

Click on the *OK* button.

The wording has changed slightly by EIMS 2.2.2; a GIF of the new dialog box is available at http://www.mail-abuse.org/tsi/graphics/eims_2.2.2_config.gif.

The information above also applies to version 1.2.1 and later of the freeware server; versions 1.2 and earlier do not have this capability.

Unfortunately, even with these measures in place, it appears that the server will accept mail for relay from anyone who forges a from address of a valid user at your server. That means any spammer could pretend to be `postmaster@yourdomain` (or any other valid user) and have the ability to use your server as a spam relay. Some testers may not accurately reflect this vulnerability, saying the sever is secured, when it is actually still insecure. If you're having problems trying to secure your copy of EIMS, we recommend that you contact Eudora for assistance.

Eudora WorldMail Server

Status: Commercial ([Qualcomm](#))
Systems: Win/NT
Info: <http://www.eudora.com/worldmail/>

As delivered, WorldMail Server version 1.0 is vulnerable to relay. There used to be a fix, but nobody can find it anymore.

Version 2.0 and above no longer have this problem, and Eudora offers free upgrades at <http://www.eudora.com/worldmail/updaters.html>.

exim

Status: Freely Available
Systems: Unix
Info: <http://www.exim.org/>

One of the strengths of the *exim* mailer is its mail filtering and processing capabilities. Recent releases have relay disabled, by default. There are several configuration options to control relaying on the basis of host, domain, and network. There is a note, <http://www.exim.org/howto/relay.html>, which describes how to setup these features.

Exim is also able to use the various MAPS filters to reduce spam directed at your users; more information is available in this howto document, <http://www.exim.org/howto/rbl.html>.

FloosieTek FTGate

Status: Commercial (Floosietek)
Systems: Windows
Info: <http://www.floosietek.com/ftgatehome.htm>

The Security tab of the FTGate Properties dialog has a Relay Control section. Select "Deny relaying to any site not listed below". These details were taken from http://www.floosietek.com/webhelp/FTGateSecurity_Properties.htm; we do not know at this time whether FTGate checks the reverse DNS of the connecting machine, or merely the envelope FROM address. If it is the latter, spammers can easily continue to relay by simply forging the FROM.

Gauntlet

Status: Commercial ([TIS](#))

Systems: Unix (we do not have information on the NT version)
Info: <http://www.tis.com/support/>

Gauntlet 4.2 UNIX requires at least SMAP Patchlevel 1.

Amend the netperm-table, using the GUI or by hand, to include your valid domains and mail relays.

Amend netperm-table by hand to include deny-route-char which stops the use of routing address like:

```
users@victims.com@validrelayed.domain  
deny-route-char *%*  
deny-route-char *@*
```

Gauntlet 5.0 and above combine this in the GUI.

Groupwise

Status: Commercial ([Novell](#))
Systems: Unix
Info: <http://www.novell.com/groupwise/>

GroupWise 5 GroupWise Internet Agent (GWIA) may be *partially* secured against unauthorized relay. This is not, however, complete relay control, and third parties may still take advantage of your system.

Using NWAdmin, go to the details page of the Gateway. Click on the "Access Control" tab, and then the "SMTP Relay" button. Check the "Prevent Message Relaying" radio button, then click OK.

There is a workaround to secure the GroupWise SMTP/MIME gateway. Edit the DOMAIN/WPGATE/SMTP/GWSMTP.CFG file (with any text editor) and add the switch "/NOROUTING". Mail relay will now be disabled. If you have the option set to save problem mail, the messages instead will be saved into your problem directory, so be sure to keep an eye on it.

In version 5.5, add "/NOROUTING" to the GWIA.CFG file in the SYS:SYSTEM folder.

We've been told that these relay control features simply do not work before version 5.5.4, and that even after 5.5.4 quoting the recipient address will bypass all of Groupwise's relay controls.

Novell has released a patch which is reported to fix the "quote hack" in 5.5.4 (aka Groupwise 5.5 with Service Pack 4.) This patch will not work on earlier versions of Groupwise, or if SP4 is not installed. It is also available from Novell's [website](#).

GroupWise 6 is now the current release. It will prevent relay messages. Using the ConsoleOne admin utility, goto the properties of the GWIA gateway. Click on the "SMTP Relay Setting" from the "Access Control" tab/menu. Under the "SMTP Defaults" box, Check the "Prevent Message Relaying" radio button, then click OK. The GWIA will restart on its own. the GWIA can now be tested for relay by following this Novell [TID](#) and using "rcpt to: test@nodomain.com". You should receive a "550 Relaying denied"

IMail Server

Status: Commercial [Ipswitch, Inc.](#)
Systems: Windows/NT
Info: http://www.ipswitch.com/products/IMail_Server/index.asp

We're told that Imail is open relay by default, but can be closed easily. To stop open relay, on the Imail SMTP Security panel, click Relay options:Relay for Addresses and enter your trusted ip addresses and/or subnets. Then, on the Imail SMTP Security panel, UNcheck "Disable SMTP AUTH reporting" and tell all your mail users to use SMTP AUTH in their mail client programs.

More information is in Chapter 8 of the [IMail 6.0 Manual](#) (PDF, 2099K.),
<ftp://ftp.ipswitch.com/ipswitch/manuals/imap6.pdf>.

InterMail

Status: Commercial ([Software.com](#))
Systems: Unix, Win/NT
Info: <http://www.software.com/products/default.htm>

See below for information on InterMail Post.Office Edition (formerly simply "Post.Office".)

InterMail Mx and Kx editions also appear to have relay control features, but documentation is only available with a support contract.

International Messaging Associates Internet Exchange

Status: Commercial ([International Messaging Associates](#))
Systems: Windows 95 and Windows NT
Info: <http://www.ima.com/>

Version 2.12 and above:

- In the Internet Exchange main screen click on Options.

- Click on Advanced
- Make sure there is a check mark next to Reject Remote Recipients
- Click on OK
- Click on OK

The Help file states, "SMTPD will reject remote Internet recipients for incoming mail. This is to prevent remote sites from trying to spoof messages by re-routing them back out through the gateway."

This product also supports filtering through the various MAPS lists.

Isode Message Switch

Status: Commercial ([Isode Ltd.](#))
Systems: Unix
Info: <http://www.isode.com/IC-6037V1.1.html>

The Isode Message Switch has a number of capabilities to prevent mail abuse, including unauthorized relay. They have published an application note, <http://www.isode.com/support/ic-8411.html>, describing how to configure these features.

In summary, you will want to setup up two different SMTP channels, a *local-smtp* channel for hosts that should be granted relay access (e.g. those on your local network), and an *external-smtp* channel for all other traffic. Then, an *auth.channel* table entry is made to block direct relay from *external-smtp* to *external-smtp*. This will prevent unauthorized hosts from relaying mail through the server, unless it passes through some other processing operation, such as list expansion.

IT House Mail Server

Status: Commercial ([IT House](#))
Systems: Windows
Info: <http://www.ithouse.com/Start.htm>

Inside the Access Filtering dialog (Properties/Mail Server Properties/Server Properties/Security/Server Access Filtering), you can create or edit various filter types. It appears that at the moment, the only relay control IT House supports is "Allow relays for local domains only." This will allow anybody whose From: address matches one of the domains you're hosting to relay; spammers are known to forge that to take advantage of such relays.

The filters also let you deny specific IP addresses from making any SMTP or POP connections, but that won't help until you know where the spammers are coming from -- and they tend to move around a lot.

At the moment, our suggestion would be to either place another mail server as a firewall in front of IT House, or change to different server software entirely.

Lotus cc:Mail

Status: Commercial ([Lotus](#); to be discontinued)
Systems: Windows
Info: <http://www.lotus.com/home.nsf/welcome/ccmail>

After much searching, somebody finally discovered that there *is* a way to secure cc:Mail. Unfortunately, it requires turning off POP and IMAP support entirely. Lotus's document describing how this works is [here](#).

For cc:Mail SMTP v8.5, a built in spam prevention configuration is available via the configuration applet located in the Control Panel entitled "Link to SMTP." Click on HOST INFO, ADVANCED, and FILTER to define the spam filter. The default option is to ACCEPT and RELAY all mail not matching any filters. Instead, change this to ACCEPT. This will prevent ccMail SMTP from being used as a mail relay by anyone (including, most likely, your own users.) In addition, you can define specific filters to immediately block any particular email addresses, domain names, etc from being sent from on this screen.

Lotus Notes and Lotus Domino (up to R5)

Status: Commercial ([Lotus](#))
Systems: Win/NT and OS/2 Warp

To disable relaying, put the line

```
SMTPMTA_REJECT_RELAYS=1
```

in notes.ini

Two more notes.ini settings which may help:

```
SMTPMTA_DENIED_DOMAINS
```

The NOTES.INI variable (SMTPMTA_DENIED_DOMAINS) allows you to enter the PATHNAME of an ASCII file containing domains that your organization wants to prevent from sending mail. If it is NULL or not present, the MTA will accept mail promiscuously.

SMTPMTA_HELO_DOMAIN_VERIFY

A NOTES.INI variable (SMTPMTA_HELO_DOMAIN_VERIFY) authenticates the domain name specified in the HELO/EHLO console command. It does this by verifying that the IP address used by a remote host is actually associated with the purported Domain Name that the host has supplied.

Note: the Hello Verify and Denied Domain Lists features may be used together or independently of each other.

A full list of ini file settings can be found at <http://support.lotus.com/sims2.nsf/802ee480bdd32d0b852566fa005acf8d/31c2a8087f9e6c938525669c0053debe?OpenDocument>, and some of the other anti-spam settings that Notes supports are described in <http://www.keysolutions.com/NotesFAQ/whatlotus.html>.

Unfortunately, these measures may not be entirely adequate. Even after these fixes are applied, it appears that some configurations of Lotus Notes/Domino will continue to relay for unauthorized third-parties, if the recipient's email address is specified in quote marks. For those of you who are SMTP savvy, that means, during the SMTP transaction, specifying the recipient address like this: **rcpt to:<"recipient@example.com">** . If you're having difficulty securing this type of server, we recommend that you contact [Lotus](#) for assistance.

Update: with Lotus Notes 4.6.1 and higher Notes 4 releases (not Notes 5), you need to add the following to the notes.ini file:

```
SMTPMTA_REJECT_RELAYS=1
SMTP_OCH_REJECT_SMTP_ORIGINATED_MESSAGES=1
SMTPMTA_RELAY_FORWARDS=1
```

Lotus Domino R5 and above

Status: Commercial [Lotus](#)
Systems: Windows

Iris (the internal developers of Notes/Domino at Lotus) wrote a series of articles on anti-spam measures for [Notes.net](#); the second article covers relay controls.

The example graphic they've included (as of March 2000) shows a scenario where you allow relay for the entire Internet, except for IP addresses between 205.0.0.0 and 205.255.255.255. We'd consider this backwards; a much safer way to go about it is to find out what IP addresses you specifically *want* to allow, put those into the "Allow messages only from the following..." field, and deny everything else.

Luckily, the product does appear to support this more effective method.

Unfortunately, these measures may not be entirely adequate. Even after these fixes are applied, it appears that some configurations of Lotus Notes/Domino will continue to relay for unauthorized third-parties, if the recipient's email address is specified in quote marks. For those of you who are SMTP savvy, that means, during the SMTP transaction, specifying the recipient address like this: **rcpt to:<"recipient@example.com">** . If you're having difficulty securing this type of server, we recommend that you contact [Lotus](#) for assistance.

LSMTP

Status: Commercial ([L-Soft International, Inc.](#))
Systems: Windows NT
Info: <http://www.lsoft.com/lsmtp.html>

To disable relaying in v1.1a (and, presumably, later) go to Relay Control, Check the "enable" box and enter in the IP#/Netmask for the machines you wish to allow. Some versions may have problems with matching; LSOFT says: "the newer builds clear the bits of the IP address that are zeroed in the mask".

Lyris

Status: Commercial ([Lyris](#))
Systems: NT, Unix
Info: <http://www.lyris.com/help/>

If Lyris is unprotected by a firewall (which is how many people handle it), you have only two other choices for closing the relay. Choice number one is to configure Lyris to use another host for all outbound email and close relaying on that host. The other choice is to turn the server off.

MailSite

Status: Commercial ([Rockliffe](#))
Systems: Win/NT, Win/95, Win/98
Info: <http://www.rockliffe.com/>

- Double-click on "security"
- Select "Accept mail for relay from these hosts"
- Make sure "specify mask list directly" is selected
- Replace * with !* -- this will enable SMTP AUTH, so that only users with valid username & password can relay through your server.

Mailtraq

Status: Commercial
 Systems: Win/95, Win/NT, Win/908
 Info: <http://www.mailtraq.com/>

Mailtraq 2.n, the current version, will by default only relay mail for hosts on the local network. Additional relay configuration is also possible via the Mailtraq Console. See <http://www.mailtraq.com/597/> for more information.

Mailtraq 1, the original version, was open to relaying by default. This can, however, be easily fixed. To do so, call up the Console (double-click the Mailtraq Icon in the system tray or in Control Panel). From the Options menu, choose the Services option. Select Mail Server (SMTP), then click the Properties button. Go to the Access Control tab, choose Option 3 ([2] and Local Area Network). Click on Edit and enter the IP address ranges for your LAN, then click on OK and enter any extra IP addresses (such as your ISPs Mail Server range, if your mail is delivered by SMTP). Finally, click the OK buttons twice to back out to the console and then close the console window.

MDaemon

Status: Commercial ([Alt-N](#))
 Systems: Win/NT
 Info: <http://www.mdaemon.com/> or <http://mdaemon.altn.com/>

Alt-N Technologies, the developers of MDAemon have put up a page listing all of MDAemon's security features at <http://www.altn.com/security/>. This includes POP before SMTP, MAPS list queries, and other useful options.

Mercury

Status: Freely Available
 Systems: Novell, Win/NT, Win/95
 Info: <http://www.pmail.com/>

The Mercury mailer is an NLM for Novell servers. Provisions to prevent unauthorized relay have been added as of version 1.40. If you are running a previous version, please upgrade.

The Mercury/32 mailer is re-designed for Windows/95 and Windows/NT. Provisions to prevent unauthorized relay have been added as of version 2.11. If you are running a previous version, please upgrade.

To disable relaying, the following text should be added to the [MercuryS] section of "mercury.ini":

```
[MercuryS]
Relay : 0
Strict_Relay : 1
Allow : 2.3.4.5 # The offsite backup (MX server)
Allow : 192.168.XXX.0 # Our local network
Allow : 192.168.YYY.5 # A single other machine we allow
```

For some older versions, that the "allow/refuse" entries under [MercuryS] must end with the line:

```
Refuse: 0.0.0.0
```

Current versions (including 1.47) reportedly do not need the Refuse: line.

Message Exchange (MX)

```
Status: Commercial (Mad Goat Software)
Systems: OpenVMS
Info: http://www.madgoat.com/mx.html
```

We're told that version 4.2 has no relay control features.

Version 5.0 and above, however, do. For version 5.1 (we're not sure about 5.0), full details are provided in the file mx_root:[doc]MX_MGMT_GUIDE.TXT. Briefly, it's:

```
MCP SET SMTP/NORELAY
MCP RESET SMTP_SERVER
```

Messageware MTA

```
Nexor Mailer 5.00
```

```
Status: Commercial (NEXOR)
Systems: Solaris 8/9 and Windows 2000/2003
Info: (lost?)
```

Nexor Mailer 5.00 is preconfigured out of the box to prevent relaying.

To enable trusted systems to relay through the Nexor Mailer it is necessary to register ip addresses or addresses in the mtatable. Trusted IP addresses are recorded in trusted-ip.loc, which is located in the usual location of <instdir>/mailer/tables/master. Entries are recorded in the form <ip address>:valid or <domain>:valid. An asterisk (*) can be used as a wildcard. Examples of entries in a trusted-ip table are shown below:

```
*.myorg.co.uk:valid
```

```
*.33.22.111:valid
```

Note: IP addresses are recorded in this table in reverse order. The example shown in Figure 82 indicates that all IP addresses beginning with 111.22.33 will be accepted. For earlier versions, the procedure is more complex. Contact the NEXOR support desk (support@nexor.com) at +44 115 9520501 for assistance.

Microsoft Exchange Server

Status: Commercial ([Microsoft Corp.](#))
Systems: Win/NT
Info: <http://www.microsoft.com/>

Versions through 5.0 are vulnerable to relay if they permit any local SMTP users. (Servers that only act as a gateway between internal non-SMTP mail and the Internet don't have relay problems.) In other words, if your Exchange 5.0 server is connected to the Internet, it WILL relay for anyone, and that cannot be stopped.

Starting with version 5.5, provisions have been made to prevent unauthorized relay. These are described in detail in an article from Windows NT Magazine, http://www.winnetmag.com/MicrosoftExchangeOutlook/Article/ArticleID/7696/MicrosoftExchangeOutlook_7696.html. If you're running an older version, it's time to upgrade.

Microsoft has an article on their [TechNet site](#) that discusses securing Exchange 2000 and 5.5.

MMDF

Status: Freely Available
Systems: Unix
Info: <http://www.irvine.com/~mmdf/>

SCO has a technical article on their web site, at <http://www.sco.com/ta/>, article number 104596, on securing their version of MMDF (and possibly all versions) against relaying.

Multinet for OpenVMS

Status: Commercial
Systems: OpenVMS

To disable relaying:

- Install latest version of Multinet - version 4.1
- Locate release notes in the multinet:[documentation] directory. Go to page 3-15.

- Extract the example file (page 3-15 onwards) to a new file which should be called MULTINET:SMTP_SERVER_REJECT.
- Edit the file as you wish, although this may not be necessary.

Netscape Messaging Server

```
Status: Commercial (Netscape Communications Corp.)
Systems: Unix, Win/NT
Info: (version 3)
      http://home.netscape.com/comprod/server_central/product/mail/
      (version 4)
      http://www.iplanet.com/products/infrastructure/messaging/n_mes
      s/index.html
```

Extensive anti-spam capability has been added with version 3.5; anyone running an earlier version needs to upgrade. Extensive third-party documentation and examples can be found here, <http://www2.tsc.com/~bobp/nms-no-relay.html>.

Netscape has also published a note, <http://help.netscape.com/kb/corporate/19980217-31.html>, that describes how to write a filter script to block unauthorized relay, but many of those examples are easily defeated.

Version 4 and above are being released in alliance with Sun and merged with the [Sun Internet Mail Server](#), and are reported to be evolving quickly.

NTMail

```
Status: Commercial (Internet Shopper)
Systems: Win/NT, Win/95
Info: http://www.ntmail.co.uk/
```

NTMail provides several anti-relay and anti-spam measures, including some sophisticated add-on options.

Recent versions of NTMail leave relaying turned off by default. For older versions, secure against unauthorized relay by selecting the "Only Accept Local Mail" option. Then enter the hosts that are allowed to relay mail through your server in the "Treat as Local" section. You can specify either domain names or host IP addresses. Use addresses if you can; names may be subject to spoofing.

For NTmail version 3 on NT 4.0, updating software from v3.006 to 3.0017 knocked out the security tab functionality without the Juice module loaded. Thus, the GUI based settings described above were not available, making it an open relay. To secure smtp, you'd instead add/edit registry key "IPAllowed" and "LocalIP" and set key "OnlyAcceptLocal" value "1".

Although upgrading to the newest version or at least using The Juice Module is a better solution than direct regedits, that may not be possible for everyone.

"IPAllowed" and "LocalIP" are space separated lists of IP address ranges. Add the values for each IP range server will relay for.

An asterisk "*" is the standard wildcard to allow any. The Exclamation point excludes, disallows the IP or wildcard after it. A question mark is a single digit wildcard. Thus, 204.152.184.* will allow Mr. Vixie's /24 and !204.152.184.74 will disallow mail-abuse.org from sending mail through server. :) Refer to the nmail documentation, for more details on expressing ranges such as "IP.32-63".

The "!" at the right most of IPAllowed will explicitly block all other IP addresses; its' use is recommended.

```
Hkey_Local_machine:SOFTWARE\InternetShopper\Mail\Parameters
:IPAllowed:REG_SZ:"204.152.184.* !204.152.184.74 !*"
:LocalIP:REG_SZ:"204.152.184.*"
```

By default, LocalIP's value was "*". That must be changed to only the IPs local to the server; and OnlyAcceptLocal's value set to 1 (true).

Notes on NTmail registry settings:

When subkey is saved as a text file, the important anti-relay settings look like:

(NTMail 3.03.0017/4c.ar3k)

In mail servers Hkey_Local_machine, When subkey is saved as a text file, the important no relay settings look like the following.

```
Key Name:          SOFTWARE\InternetShopper\Mail\Parameters
Class Name:
Last Write Time:   5/24/00 - 10:00 PM
```

...

```
Value 4
Name:      IPAllowed
Type:      REG_SZ
Data:      our.IP#.c1.* our.IP#.c2.* our.IP#.c3.* !*
```

```
Value 9
Name:      LocalDomainNames
Type:      REG_SZ
Data:      example.com *.example.com
```

```
Value 10
Name:      LocalIP
Type:      REG_SZ
Data:      our.IP#.c1.* our.IP#.c2.* our.IP#.c3.*
```

Value 15
 Name: OnlyAcceptLocal
 Type: REG_SZ
 Data: 1

3.02.xxxx is *not* securable against relay. 3.03.0018 (also called 3.03e) is secure by default and without the installation of the Juce add-on. 3.03e is a free upgrade from 3.02.xxxx, insofar as the same key can be used. 3.03e also fixes some denial of service attacks in previous builds. When upgrading, you may need to go and enable relay protection manually.

Obtuse smtpd

Status: Open source ([Obtuse](#))
 Systems: Unix
 Info: <http://www.obtuse.com/smtpd.html>

Obtuse smtpd is part of the Juniper firewall toolkit. The newer version 2 includes filtering options to limit relaying. This *may* still allow % relaying, but there are tools which allow you to block any message with the % character in the address.

The documents (both the man page and the address check instructions) are done with an eye towards filtering, and appear pretty easy to use.

pmdf

Status: Commercial ([Innosoft International](#))
 Systems: Unix, OpenVMS
 Info: <http://www.innosoft.com/>

Version V5.1-7 of this product has capabilities to stop unauthorized relay. In fact, Innosoft has published an application note called "Preventing SMTP Relaying Through PMDF", http://www.innosoft.com/app-notes/spam_toc.html.

Postfix

Status: Open source (postfix.org)
Systems: Unix
Info: <http://www.postfix.org/>

Postfix is not, by default, an open relay. More information (including explanations of some confusion behavior in early versions) can be found in the Postfix FAQ, http://www.postfix.org/open_relay, and the UCE Controls, <http://www.postfix.org/uce.html>, section of the Postfix Configuration manual.

Post.Office

Status: Commercial ([Software.com](http://software.com)); renamed "InterMail Post.Office Edition"
Systems: Unix, Win/NT
Info: <http://www.software.com/products/impostoffice.html>

Instructions for relay control in Version 3.5, software.com will warn you that you should only edit these settings if you are experienced, but if you've gotten this far then you're clearly experienced enough to point and click. For true relay security, we suggest choosing the "In general, restrict relay mail except as indicated below" option and then entering the IP addresses which should be permitted to relay. Simply choosing "Local Mail Domains" may feel good, but spammers know they can get around that by forging your domain into their mail before sending it.

There's also a PDF entitled "Suggested Anti-Relay Settings for InterMail Post.Office Edition".

For version 3.1, The [instructions](#) are in section 3 of the release notes. Pull up the "SMTP Relay Restrictions Form." Select the "Restrict relay mail except as indicated below" setting. Then enter the hosts, networks, and domains that are permitted to relay through your server.

The good folks at DictaComm Services INC. have put together a quick checklist for closing relay on Post.Office 3.x, available at http://www.dictacomm.com.com/HOW_DO/postoffice.htm.

Qmail

Status: Freely Available
Systems: Unix
Info: <http://www.qmail.org/>

qmail prohibits relay by default, since version 0.91. The [*qmail-smtpd*](#) daemon will consult the *rcpthosts* control file to determine valid destination addresses, and reject anything else.

The issue here is not how to disable third-party relay, but rather how to permit relay access by authorized hosts. This is answered in the *qmail* FAQ, <http://www.qmail.org/qmail-manual-html/misc/5.4>. It describes a method that allows you to grant relay access to certain hosts or networks.

Russell Nelson has an alternative solution, <http://www.qmail.org/open-smtp.tar.gz>, that grants relay access to users with valid POP3 accounts, regardless of the network address they come in on.

QuickMail Pro Mac 1.1.1r1 Server

Status: Commercial
Systems: Mac
Info: <http://www.cesoft.com/>

Servers that support mail relaying can accept and deliver incoming messages intended for non-local addresses. This capability can be extremely valuable if you want one server to distribute mail for many people from various domains. It can also be a drawback due to the unsolicited bulk E-mail (junk mail) that often overloads Internet servers.

QuickMail Pro Server has controls that can reduce the amount of mail routed through your server so your LAN users have the fastest mail possible. To reduce mail flow on your Internet mail server:

- Select Domain Setup in the Configure menu.
- Double-click the SMTP domain entry in the Domain Setup window.
- Select your mail relay options in the Relaying box of the SMTP Domain dialog and click OK.

QuickMail Pro Windows (95/NT) 1.5 Server

Status: Commercial
Systems: Windows 95 and NT
Info: <http://www.cesoft.com/>

Servers that support mail relaying can accept and deliver incoming messages intended for non-local addresses. This capability can be extremely valuable if you want one server to

distribute mail for many people from various domains. It can also be a drawback due to the unsolicited bulk E-mail (junk mail) that often overloads Internet servers.

QuickMail Pro Server has controls that can reduce the amount of mail rerouted through your server so your LAN users have the fastest mail possible. To reduce mail flow on your Internet mail server:

- Select the Relay Filtering tab.
- Click Enable Relay Filtering.
- Choose which server you want to relay mail for by clicking Add in the Allow box. Click OK.
- Select Single Machine or Address Range and type the IP address of the machine(s) for which you are relaying mail.
- Click the Edit button in the Enter an IP Address dialog if you don't know the machine's IP address to display the DNS Address dialog. Type the DNS Name at the prompt. Click OK to return to the Enter an IP Address dialog.
- In the Relay Filtering tab, choose which server you want to restrict mail for in the Restrict box. Select the Restrict All check box to eliminate mail relaying for all other sites.
- Click Apply.

Note: If you are using Windows 95, you must restart the server for the filtering changes to take effect.

rblsmtpd

Status: Freely available (experimental)
Systems: Unix
Info: <http://pobox.com/~djb/rblsmtpd.html>

rblsmtpd should work with any UNIX system with an SMTP server. It supports RBLSM text in SMTP, fast timeouts, local RBLSM protection, and two "fail secure" options.

Seattle Lab SLMAIL

Status: Commercial ([Seattle Lab](#))
Systems: NT 4.0
Info: <http://www1.seattlelab.com/slmail/>

Recent versions offer anti-relay filters and other anti-spam features. Documentation available at <http://docs.seattlelab.com/slmail.asp>.

Sendmail Version 5

```
Status:  OBSOLETE
Systems: Unix
Info:    unknown
```

Sorry. You are running an obsolete mailer. It has no known solution to prevent relay. Moreover, your mailer is rife with security holes. Unauthorized relay is the least of your worries. Your mail system is in serious jeopardy, and you should consider planning your upgrade to a modern mailer.

Sendmail Version 8

```
Status:  Freely Available
Systems: Unix
Info:    http://www.sendmail.org/
```

Versions before 8.8.4 require serious configuration hacking, and even then they aren't totally secure. Time to upgrade.

Rulesets for version 8.8.x are available from Claus Aßmann's web site at [sendmail.org](http://www.sendmail.org/~ca/email/check.html), <http://www.sendmail.org/~ca/email/check.html>. There are others around, but Claus's tend to be updated the most frequently.

Many sites which run 8.8.x have added anti-relay configuration, but are still susceptible to the "percent hack." Please pay special attention to the `removelocal` portion of `check_rcpt` in Claus's recipes to fix that.

Another approach is to limit mail server access to only those users who have authenticated themselves with a POP password, <http://spam.abuse.net/adminhelp/smPbS.shtml>. This is the so-called POP-before-SMTP solution. Although this is more complicated to setup, it is an excellent solution for providers that have "roaming users."

ISPs that are members of the [iPass](http://www.ipass.com) network should email ask@ipass.com to obtain the "Anti-Spam Kit" for sendmail 8.8.

Starting with version 8.9.0, *sendmail* prohibits relay by default, and provides a number of parameters to control this feature. See the [Anti-Spam Configuration Control](#) section of the *cf/README* file for information on these settings.

Caution: Most of these solutions require you to setup a list of domains to which relay is allowed. Be sure to include all authorized domains in this list. Don't forget downstream domains for which you MX, as well as virtual domains that you serve. Otherwise you will begin rejecting mail that you shouldn't.

Another caution: if you have configured sendmail 8.9.3 with `FEATURE(relay_entire_domain)`, this will accept relays from any host in your domain. What's "your domain"? It's your host name with the first "word." stripped from it. Unfortunately, by default, sendmail checks *EVERY* IP address on your system and does reverse lookups.

Many systems have a default as-shipped 'localhost.rev' that has 127.0.0.1 point to localhost.berkeley.edu or something like this. This means that any host in berkeley.edu will be able to relay, but your own hosts may be rejected. There other services that rely on your server having correct reverse DNS as well, so it'd be a good idea to fix this.

Many, many, systems have at least one virtual host where the reverse DNS just points to the domain name, e.g., xxxstuds.com or some similar thing. This is where you end up with an open relay; such a machine will relay for anything in '.com'. Similarly, if you had a virtual host (or even just your main IP) resolving to 'example.net', you would discover that anything in '.net' was allowed to relay.

The best solution is to upgrade (including the .cf file); if for some reason you can't do that, specify relay hosts by IP address instead of using `relay_entire_domain`.

Sendmail Pro

```
Status: Commercial (Sendmail)
Systems: Unix, Win/NT
Info: http://www.sendmail.com/
```

This commercial version of sendmail should have the same relay control features as the free, open source [sendmail 8.x](#), plus a graphical interface intended to make configuration easier and all sorts of technical support options.

Smail

```
Status: Freely Available
Systems: Unix
Info: http://www.sbay.org/smail-faq.html
```

smail version 3.2 has support to block unauthorized relay. This is enabled by defining the `smtp_remote_allow` parameter in your *config* file. Set it to the list of local IP address ranges from which unrestricted relay is allowed. All other hosts will be refused.

Smail version 3.1 is vulnerable to relay. It also has some well-known security problems. The authors suggest that you upgrade to either version 3.2 or [exim](#).

SmartMax MailMax

Status: Commercial ([SmartMax](#))
Systems: Windows
Info: <http://www.smartmax.com/mailmax.html>

As of version 3.0, it appears that MailMax has no effective relay control features. Though there is a checkbox to only allow relay from local domains, that won't stop spammers from forging your domain and then relaying all they please.

Stalker Internet Mail Server (SIMS)

Status: Commercial Freeware ([Stalker Software](#))
Systems: Mac
Info: <http://www.stalker.com/SIMS/>

Current versions of SIMS prohibit unauthorized relay through your mail server. Starting at version 1.2, unauthorized relay detection is implemented at the protocol level. If your version is older, please download the current release, <http://www.stalker.com/SIMS/Current>.

The instructions to restrict unauthorized relay are provided on the SIMS web site, <http://www.stalker.com/SIMS/Relay>. You will need to open the "SMTP Service Settings" and click the "Client Hosts" button. Then, enter the range of host IP address that should be allowed to relay mail through your server.

Sun Internet Mail Server

Status: Commercial ([IPlanet](#))
Systems: Solaris
Info: <http://www.iplanet.com/products/infrastructure/messaging/sims/index.html>

Version 4.0 and above are being somehow merged with [Netscape Messaging Server](#) and released under the name IPlanet.

Symantec Norton Anti-Virus for Gateways

Status: Commercial ([Symantec](#))
Systems: NT
Info: http://www.symantec.com/nav/nav_ieg/

We're told that version 1.x simply cannot be secured against relay, even when configured to simply forward all mail to a server inside the firewall. Symantec has fixed with version 2.x.

Previously, the MAPS had suggested against use of version 2 as well, due to what we're told was incorrect information in Symantec's knowledge base. They've now updated that information, and it appears that Norton Anti-Virus 2.x has all the anti-relay functionality we'd expect from a well-designed product.

TFS Gateway

Status: Commercial ([TenFour](#))
Systems: Win98, WinNT
Info: <http://www.tenfour.com/Gateway/index.htm>

TenFour reports that TFS Gateway will accept the mail (thus failing most automated relay tests), but will generate an error message and won't forward the message on.

If you are using 4.6, you can add Verify=ON under [SMTP] in tfs3.ini, and then it won't even be accepted.

TIS FireWall ToolKit (FWTK) smap/smapi

Status: Unclear ([FWTK.ORG](#))
Systems: Unix
Info: <http://www.fwtk.org/>

Though TIS (now owned by Network Associates) does not appear to have implemented relay control in new releases, there are a number of third-party patches that should solve the problem, <http://www.fwtk.org/fwtk/patches/2.2>.

Vircom VOPmail

Status: Commercial ([Vircom Online](#))
Systems: Windows
Info: <http://www.vircom.com/vopmail/>

VOPmail appears to be one of those that we'd call "best of breed" -- it not only implements basic relay control, it also supports SMTP AUTH and even lets you do RBL queries.

VM/CMS

Status: Commercial
Systems: VM/CMS
Info: <http://risc.ua.edu/pub/network/vm/>
Info: <http://nsl.tusc.net/pub/network/vm/>

Pascal source for code closing relaying and placing the incoming IP address on the "Received" line of a VM/CMS system is available at the above URLs.

VM/ESA TCP/IP

Status: Commercial ([IBM](#))
Systems: AS/400
Info: <http://www.vm.ibm.com/related/tcpip/spamming.html>

That is all the information we have at this point.

VM SMTP

Status: Commercial ([IBM](#))
Systems: IBM VM
Info: <http://www.vm.ibm.com/related/tcpip/>

If you're running FL310 or V2R4, there is an APAR available which allows you to control who may relay through your server (they call it "forwarding," which has a different meaning in common Internet terminology.) Information is here, <http://www.vm.ibm.com/related/tcpip/spamming.html>.

There do not appear to be any relay controls for earlier versions.

ZMailer

Status: Freely Available
Systems: Unix
Info: <http://www.zmailer.org/>

There are policy control (<http://www.zmailer.org/smtp-policy.html>) features that you can enable to stop unauthorized relay. You will need to setup an *smtp-policy.relay* file listing the hosts and networks that are authorized to relay outbound mail through this server, and an *smtp-policy.mx* file listing the additional domains for which you are willing to accept incoming mail. Then, run the *policy-builder.sh* to generate the specified filtering policy.

