Use of RBLs - Realtime Blackhole Lists

iQ.Suite Tips & Tricks for IBM Domino

RBLs or DNS-based blackholes (DNSBLs) are blacklists which can be queried in realtime on suitable, dedicated internet servers for the purpose of classifying emails of dubious origin as spam. The majority of RBLs contain the IP addresses of computers from which spam has been sent in the past. Nowadays, these computers are generally open mail relays or trojanised PCs which have been tampered with by spammers.

The Domino server can be used to evaluate these lists virtually in realtime via the DNS protocol whenever an email comes in. If the result is positive, the email can be rejected or tagged. The advantage of tagging lies in the option of filtering the emails via the iQ.Suite and placing them in quarantine in the first instance. This means that emails with correspondents who may find themselves blacklisted cannot be lost:

How to configure the DNSBL query on the Domino server activate the DNS blacklist filter in the respective configuration document under:

"Router/SMTP"
"Beschränkungen und Steuerungen" / "Restrictions and Controls"
"SMTP-Eingangsteuerung" / "SMTP Inbound Controls"

Enter the BL server(s) of your choice and select "Prokollieren und Nachricht markieren" / "Log and tag message"

You can choose from a wide range of publicly available and private, paid subscription services, all of which manage DNS blacklists. You should limit the number of sites you choose for performance reasons, as Domino performs a DNS lookup to each site for every connection. Please consult the website of the respective provider for information on options and offers (in the example http://www.spamhaus.org/zen/).
Domino now performs a DNS query of the blacklists on the specified sites for every incoming SMTP connection.

If Domino finds a match for a connecting host in a blacklist, the Notes field "$DNSBLSite" is added to the messages in question (along with the respective console messages and entries in the Notes protocol). A $DNSBLSite field contains the blacklist site on which the host was found.

Please consult the Domino server documentation provided by the manufacturer for more details on this functionality in Lotus Domino.

The iQ.Suite formula rule "RBLListedSender" queries the presence of this field:
You can copy the sample job "SAMPLE - Block Domino DNSBlacklist Entries" (priority 7150) and activate it once you have performed the steps listed above. Adapt it to suit your requirements if necessary. You could, for example, add your whitelists to the dependence on negated rules list, modify the priority or specify that emails should not be deleted in the first instance in order to obtain an overview of behaviour without your users noticing.

All emails to which the Domino server has added the Notes field "$DNSBLSite" will be recorded by this job and the actions defined under "Operations" performed. Please make sure that you have configured an entry under "Misc." - "Quarantine configuration". The default entry is "DEFAULT - Quarantine configuration". In this case, both the email and associated report are stored in the default quarantine database g_arch.nsf.

Those fighting the battle against spam often have the impression that they are tilting at windmills.
Spammers are always changing their tactics, rendering yesterday's solution obsolete and necessitating yet another foray into spam technologies. The iQ.Suite provides flexible anti-spam solutions which only have to be configured once and can then be left as they are or, just occasionally, readjusted very slightly. Our new Avira product "Avira Space", the Sophos Antispam Interface (SASI), CORE and RBL are capable of adapting dynamically to constantly changing spam technologies without having to be updated regularly by the administrator.

In our training courses, we gradually develop a multi-level anti-spam concept tailored to your requirements, which restores time and space for important everyday concerns to both you and your users alike.

Why not visit us? We look forward to meeting you!