Allow and deny lists

Allow and deny lists

- All Janet services are governed by the Janet policies [1].

Janet has its own copies of the following leading allow and deny lists:

- Spamhaus Zen lists [2]
- URIBLs [3]
- DNSWL.org [4]

DNS deny lists are a well-established technique. They identify sources of e-mail abuse as lists of IP address blocks, enabling Janet organisations to quickly and easily reject a high proportion of unwanted e-mail.

Allow lists contain all currently known good email servers, and are the opposite of deny lists, mail from the allow listed e-mail addresses, domains, and/or IP address should generally be allowed. Using Allow lists and deny lists assists in blocking unwanted messages while allowing wanted messages to get through. E-mail allow lists are used to reduce the incidence of false positives and to speed up the filtering process, as they are often based on the assumption that most legitimate mail will be from a relatively small and fixed set of senders.

Unlike most deny lists, URIBLs are not lists of message senders but URLs (Web addresses, some but not all representing undesirable sites) which have been seen in e mail messages identified as spam or phishing, or are otherwise dangerous. Links seen in such messages tend to be more stable than the rapidly changing botnet IP addresses used to send the vast majority of them. The Spamhaus sender lists can be used in a first stage filter and the URIBL lists can help in a second stage filter to find many of the otherwise difficult, remaining unwanted messages.

If you think that a Janet DNSBL is affecting the delivery of your e-mail messages, please read this page:

- What to do if your mail is being blocked [5]

Display as Single Column?:

What to do if your mail is being blocked

What to do if your mail is being blocked

If you are outside Janet and you believe a Janet organisation is blocking mail from you, please read this note before recording a complaint.

A Janet mail server is blocking me. Why?

Many Janet organisations use the Janet DNS deny lists (Spamhaus Zen) to refuse mail connections from listed IP addresses. Janet endorses this use but does not manage the content of the lists concerned.

To find whether your mail server is on the list, fill in its IP address at

http://www.spamhaus.org/sbl/index.lasso [6] (for SBL, XBL, PBL, Zen)

What can I do about it?

You should be able to tell from the above lookup pages which of the lists and component lists you are on. The criteria for listing, and the action you should take, are summarised later in this note (*Component lists***).**

What can Janet do about it?

Janet encourages customer organisations to use the Spamhaus Zen lists. If you believe you are prevented from sending mail because you are listed there (or in the Janet Zen lists which are our replicas), our advice to you is to follow the instructions for the list concerned.

Note that there may be a delay of up to an hour between removal of an entry from the Zen lists and its disappearance from the Janet replica.

If you believe your IP address is not listed and a Janet customer organisation is refusing email from you for some other reason, please contact the Janet Service Desk. [7]

Other causes of email blocking.

Janet provides mirrors of selected DNSBL's, but individual customer organisations are free to make their own choices about which lists they use, and about domains or IP addresses from which they do not wish to accept email.

Many other DNSBLs are available, each with their own criteria for listing and removal from the list

Component lists

Spamhaus

- **SBL** (Spamhaus Block List) lists the IP addreses of direct UBE sources, spam services and spammers themselves. Anyone on SBL will have to demonstrate that they now follow good practice.
- **XBL** (Exploits Block List) lists addresses which are victims of illegal third party exploits,

including proxies, worms and trojan exploits. Ensure that your computer or computers are clean of infection and not under the control of an unauthorised third party.
- **PBL** (Public Block List) lists IP address ranges whose owners' policy is that they are not expected to be used directly for outbound email. The IP address of your mailer is in a service provider's consumer facilities and it is not expected to connet directly to other people's mail servers. Either send mail through your service provider's outgoing server (possibly called their "SMTP server" or "smarthost") or ask your own service provider for help.
- **DBL** (Domain Block List) lists host and domain names used as references within the body of spam messages. This list can be used in conjunction with email content scanners to help detect spam.

Zen is the union of SBL, XBL and PBL; IP addresses are in Zen if and only if they meet the criteria for one or more of the other three.

Further information

Spamhaus pages:

- http://www.spamhaus.org/ [8]
- Look up an IP address: http://www.spamhaus.org/sbl/index.lasso [6]

One of several lists of other address lists:

- Declude: http://www.declude.com/Articles.asp?ID=97 [9]

Display as Single Column?:

The Spamhaus Zen lists in Janet

The Spamhaus Zen lists in Janet

The Spamhaus Zen lists in Janet

Janet makes available to all organisations with a Janet connection a maintained copy of the Spamhaus lists SBL, XBL and PBL, and the Zen list which is the union of those three. This document is for the information and guidance of those who manage or administer e-mail services within Janet organisations.

If you think Janet is blocking your mail

If you are outside Janet and you believe a Janet organisation is blocking mail from you, please read the short separate note "What to do if your mail is being blocked [10]" before recording a complaint.

In the rest of this document:

- **How to use the Janet Spamhaus lists**

How to use the Janet Spamhaus lists

Modern mail server programs have facilities for polling DNSBLs (*DNS deny lists*) at various stages in the SMTP protocol, and they will usually 'reject' transfer attempts from listed IP addresses. Most of them include lookups from the standard Spamhaus domains or others in their default configuration.

If your organisation has a Janet connection and wishes to use SBL and the others, you need only to set the zone where the lookups are made to
zen.dnsbl.ja.net
according to the documentation for your own e?mail server product.

That documentation will provide detailed instructions (which file to edit, or which menu or command to use). Later in this document are some outline examples (see *E-mail server products* below).

Configuration for use outside Janet uses the zone
zen.spamhaus.org
which may be referred to in the server documentation or included in the standard configuration.

In the Janet zones the first component of the zone is unchanged (sbl, xbl, pbl or zen); note that the deprecated combined zone "sbl-xbl" is not available and should normally be replaced by "zen".

Conditions of use

Eligibility and charges

There is no charge to organisations with a Janet connection for use of the Janet zones in dnsbl.ja.net.

For their own published zones in spamhaus.org, Spamhaus themselves reserve the right to restrict direct access. They may require heavy users to set up a transfer arrangement, for which their distribution contractors make a charge.

Risks

Use of DNSBLs carries some risks and responsibilities. Janet's view is that for most Janet organisations the likely benefit (mainly through the substantial amount of Unsolicited Bulk E-mail rejected) justifies the possible drawbacks, but each organisation must make its own choice.

- If you reject mail transfer attempts, you will delay the delivery of some mail you or your

users might have wanted. The amount should be small, but there may be a user support issue.
- Specifically, some of your own users may want to send mail through your servers (and perhaps using your e-mail addresses) from the networks of their consumer ISPs. Such networks may well be included in PBL, which is not in itself a suggestion that they are unsatisfactory. If you wish to support this practice by your users you will need to give certain IP address ranges special treatment.
- Some organisations may express irritation that you are blocking mail from them.
- Application of one or more DNSBLs does not block all unwanted mail. If you notice specific addresses from which you get a lot of unwanted traffic, you should consider adjusting your own firewall or e?mail server rules.

Protecting Janet resources

You MUST take whatever precautions are necessary to prevent access through your network from outside Janet.
Specifically, the DNS resolvers under your control MUST NOT accept recursive DNS queries from outside your own network for data in the zones within dnsbl.ja.net. Note that it is ordinary good practice to prevent all such recursive lookups from outside.
The Janet operators will record the IP address of each resolver (or perhaps e?mail server) making lookups from the zone, and will test it from time to time to confirm that it correctly rejects recursive queries.

- If it does indeed reject them, no action will be taken and it will be allowed to continue to lookup data from the zone.
- If it permits access which it should not, the Janet operators will attempt to contact the person responsible for the IP address concerned, and will then help them to correct the faulty configuration. They may suggest workarounds if it proves difficult.
- If for any reason it is not possible to implement a secure arrangement within a reasonable period, the operators will bar access to the zones from the IP address concerned.
- If you believe you may have been barred, contact the Janet Service Desk by telephone or e?mail (details at URL below).

Some networks may include DNS forwarders for internal use which are not themselves resolvers and are not the DNS clients known to the Janet nameservers. It is the responsibility of the organisation operating such a forwarder to ensure that it is not available for use from outside Janet; again, normal good practice is to make such a forwarder accessible only from within your own network.

How DNSBLs work

DNS deny lists are a well-established technique. To find whether an IP address is listed construct a special domain name from it, use an ordinary lookup for that domain name in the standard Domain Name Service (*DNS*), and see whether or not the lookup query succeeds.

To look up an IPv4 address *a.b.c.d* (in the usual 'dotted-quad' notation) in the Janet XBL, for instance, attempt to find an A (Address) record for the domain name
d.c.b.a.xbl.dnsbl.ja.net
which begins with the target address in reverse order.

If the lookup succeeds, *a.b.c.d* **is** in the Janet XBL. *127.0.0.2* is a test address included in most DNSBLs:
> nslookup 2.0.0.127.xbl.dnsbl.ja.net
Name: 2.0.0.127.xbl.dnsbl.ja.net
Address: 127.0.0.4
The address returned may give some additional information (see *Component Lists* below).

If the lookup fails, *a.b.c.d* **is not** in the list:
> nslookup 66.157.62.193.xbl.dnsbl.ja.net
Can't find 66.157.62.193.xbl.dnsbl.ja.net: Non-existent domain

Although it is quite possible to carry out manual lookups, it is expected that a mail server will automatically check each IP address from which it receives an attempt to transfer mail, and will respond to the attempt in a manner set by the system administrator and depending on the result of the lookup.

What is available

The Janet Spamhaus lists are in the four zones

sbl.dnsbl.ja.net

xbl.dnsbl.ja.net

pbl.dnsbl.ja.net

zen.dnsbl.ja.net

The nameservers for those zones can be found from the DNS in the usual way; they are reachable from anywhere in Janet but not from outside.

Janet organisations can test whether an individual IP address is in any or all of the Spamhaus lists by lookups in one or more of those zones.

Component lists

The three Spamhaus lists SBL, XBL and PBL differ in their criteria for the inclusion of an IP address. Detailed descriptions are given in the Spamhaus Web pages, but in outline:

- SBL (Spamhaus Block List) lists the IP addresses of direct UBE sources, spam services and spammers themselves.
- XBL (Exploits Block List) lists addresses which are victims of illegal third party exploits, including proxies, worms and trojan exploits.
- PBL (Policy Block List) lists IP address ranges whose owners' policy is that they are not expected to be used directly for outbound e?mail.

As well as simple success and failure of lookups, indicating only whether or not the address queried is present in the list, the address returned in the case of success gives information on the source of the data:

- SBL
  127.0.0.2 Information maintained by Spamhaus
- XBL
  127.0.0.4 Address detected on CBL
  127.0.0.5 Information based on NJABL
  (CBL and NJABL are separate DNSBLs with their own criteria)
- PBL
  127.0.0.10 Information supplied by ISPs on their own address ranges
  127.0.0.11 Information maintained by Spamhaus

Zen is the union of the three separate lists, and will succeed for an IP address included in any one or more of the three. It will then return one or more A (Address) records, each with one of the addresses above, indicating which of the component lists the queried address appears in.

Some server products can be configured to make a single query to the Zen list and use the information in these returned addresses so as effectively to treat the individual component lists separately (and perhaps send different responses depending on the source of the data). Such processing can reduce the number of DNS queries. It is otherwise possible to configure the component lists (and the responses to them) separately so that multiple lookups may be needed; or to use the same action and response for the whole of the combined Zen list.

TXT records

The zones also have a TXT (Text) record for each entry, containing material for the message accompanying the SMTP rejection code (Simple Mail Transfer Protocol, set out in RFC 2821).

The text says which list the IP address was found in, and is intended to be suitable for an e-mail server to include as diagnostic text with a failure return code. The e-mail server can retrieve the TXT record in a second lookup if desired, although some operators prefer to use a static diagnostic such as
"5.7.1 Delivery not authorized, message refused" (following RFC 3463),
or one using local wording.

Technical arrangements within Janet

Performance

Janet synchronises its replica of the DNSBL zones every 30 minutes and makes them available through several nameservers dedicated to this application. Normal use of the DNS will share load between the nameservers.

For a very short period during the update of each individual server, zone data may not be available from it or may be delayed. The Janet nameservers are managed so that the

process is completely transparent to client resolvers and service is delivered without interruption.

Access control

To ensure that Janet resources remain available to Janet organisations, the zones are served by dedicated nameservers, configured to respond only to queries which come from within Janet. Resolvers within Janet that have been seen to be using the lookup service are checked to ensure that they do not forward requests from outside Janet.

Bulk transfers

The Janet service allows unlimited lookups but there is no facility for an organisation to maintain its own copy of the DNSBLs for local querying. It is open to any organisation to make separate arrangements with Spamhaus for a direct feed of their data (for which they would make a charge).

Robustness and availability

With multiple nameservers located at different points in the network and multiple points of access to the Spamhaus data, there is no major risk to the service from equipment or network failures of other than catastrophic scale or duration.

Capacity

Load on the nameservers is continuously monitored. We believe that overload would result in performance degradation rather than a gross loss of service.

E-mail server products

These are skeleton procedures or fragments of configuration and should be read together with the documentation for each product. Each refers to the use of SBL and XBL in separate lookups, for illustration only. Most Janet organisations will be able to use Zen alone.

Exchange 2003

Exchange 2003 supports DNSBLs without additional software, through configuration items which Microsoft call "connection filtering".

To use SBL and XBL you might configure two connection filters with:

Display name *'Janet SBL'*
DNS Suffix of Provider *'sbl.dnsbl.ja.net'*
Custom Error Message *'$0 in sbl.dnsbl.ja.net'*

Display name *'Janet XBL'*
DNS Suffix of Provider *'xbl.dnsbl.ja.net'*
Custom Error Message *'$0 in xbl.dnsbl.ja.net'*

Alternatively you could pick out the SBL results and the XBL results with a single filter for the combined Zen list:

Display name *'Janet SBL?XBL'*
DNS Suffix of Provider *'zen.dnsbl.ja.net'*
Custom Error Message *'$0 in sbl.dnsbl.ja.net or xbl.dnsbl.ja.net'*
Match Filter Rule to Any of ... '2, 4, 5'

Details are at:
http://support.microsoft.com/kb/823866 [11]

Exim

In the ACL section of the configuration file there will normally be a specification for *'acl_check_rcpt'*, which can include DNSBL tests as follows:

begin acl:
 # (possibly other ACLs)
acl_check_rcpt:
 # (other rules as documented)
deny message = $sender_host_address in $dnslist_domain\n
$dnslist_text
dnslists = sbl.dnsbl.ja.net : xbl.dnsbl.ja.net
 # (rules for other DNSBLs, may be deny or warn)
accept
 # (other ACLs)

Endless variations are possible; for instance, using the single combined list Zen will reduce the number of DNS queries made, but the ACL configuration is more complicated.

A summary is at:
http://www.exim.org/howto/rbl.html [12]
and in the PDF documentation at
http://www.exim.org/exim-pdf-current/doc/spec.pdf [13]
the relevant section is the one on *Access control lists*.

Postfix

In version 2.x the normal configuration is to include DNSBL tests in the *'smtpd_recipient_restrictions*' list of the main configuration file:

default_rbl_reply = $client_address in $rbl_domain
smtpd_recipient_restrictions =
 # Following line to enable allow listing of postmaster, etc
check_recipient_access hash:/etc/postfix/recipient_checks,
 # (other restrictions as required)
reject_rbl_client sbl.dnsbl.ja.net,
reject_rbl_client xbl.dnsbl.ja.net
 # (other restrictions as required)
permit

Postfix documentation is at
http://www.postfix.org/ [14]

qmail

There is no DNSBL facility within qmail itself, but the associated programs *tcpserver* and *rblsmtpd* can manage connections to qmail. The core of the configuration is
rblsmtpd -r sbl.dnsbl.ja.net -r xbl.dnsbl.ja.net qmail-smtpd

Additional options are available, and scripts to start the various elements in sequence. Note that *rblsmtpd* looks up TXT records in the Zen lists as the basis for its decisions, not A records.

qmail documentation is available at
http://qmail.virginmedia.com/top.html [15]
For a more tutorial approach, see
http://www.thedjbway.org/djbrbl/rblsmtpd.html [16]

sendmail

DNSBL lookups are one of many 'FEATUREs', which are commonly grouped together in the configuration file.

FEATURE(`dnsbl', `sbl.dnsbl.ja.net',
`$&{client_addr} " in sbl.dnsbl.ja.net"')
FEATURE(`dnsbl', `xbl.dnsbl.ja.net',
`$&{client_addr} " in xbl.dnsbl.ja.net"')

Documentation is at
http://www.sendmail.org/doc/ [17]

Appliances

A great variety of 'e-mail security appliances' are available, some of which can use the Janet DNSBLs; others have proprietary or private lists. There are too many such devices to maintain a satisfactory list.

Other software tools

SpamAssassin users with the URIDNSBL plugin will probably wish to modify their configuration to check URIs against the Janet SBL zone, overriding the defaults:

 # Use SBL from Janet zone:
uridnsbl URIBL_SBL sbl.dnsbl.ja.net. TXT

MailScanner users may find it convenient to place the above line in
spam.assassin.prefs.conf
which should be linked from the name *mailscanner.cf* in the *site_rules* directory.

Spamhaus

The Spamhaus project is the global leader in intelligence and business pressure on those whose businesses are based on e?mail abuse. Resources for the operation come from the individuals involved and from businesses in the Internet industry who contribute hardware, infrastructure and the time of some of their staff. The project operates on a not?for?profit basis and the charge for delivery of DNSBL data merely covers the costs of the delivery operation.

The Spamhaus Web site, and specifically the Register Of Known Spam Operations (ROKSO) within that site, identifies businesses and individuals involved in bad bulk e?mail practice and documents their behaviours and relationships. The DNSBLs are a means by which e?mail providers can use that and related knowledge to make it more difficult for abusing businesses to continue their practices; they are widely used and express consensus among providers. Janet is not an e?mail provider (except in a few special cases) but most organisations with a Janet connection are.

Janet endorses the use of the Spamhaus DNSBLs for use by any organisation with a Janet connection which considers that the criteria for the lists and the likely impact on senders and local users are appropriate. It is an opportunity for Janet organisations to manage the UBE they receive and at the same time to gradually make UBE less acceptable in the worldwide Internet.

Other organisations operate or have operated DNSBLs with different criteria; although valuable in some circumstances, few have achieved the same level of acceptance as the Spamhaus lists, or before them the MAPS lists which Janet also endorses.

Further information

Spamhaus Web pages:

- **http://www.spamhaus.org/** [8]

Janet pages:

- **Janet Service Desk (for any questions)** [7]
- **For people outside Janet "**What to do if your mail is being blocked [10]**"**

E mail server products:

- **Exchange**
  http://support.microsoft.com/kb/823866 [11]
- **Exim**
  http://www.exim.org/exim-pdf-current/doc/spec.pdf [13]
  http://www.exim.org/howto/rbl.html [12]
- **Postfix**
  http://www.postfix.org/ [14]
- **qmail documentation (in UK)**
  http://qmail.virginmedia.com/top.html [15]
- **Sendmail documentation**
  http://www.sendmail.org/doc/ [17]

- **SpamAssassin**
  http://spamassassin.apache.org/ [18]
- **MailScanner**
  http://www.mailscanner.org.uk/ [19]

Others:

- **RFC 2821 Simple Mail Transfer Protocol, the standard for Internet e?mail exchange**
  http://ietf.org/rfc/rfc2821.txt [20]
- **RFC 3463 Enhanced Mail System Status Codes, which may be returned in response to attempted e-mail actions**
  http://ietf.org/rfc/rfc3463.txt [21]
- **RFC 1034, RFC 1035 and many later RFCs specify how the Domain Name System (DNS) operates**
  http://ietf.org/rfc/rfc1034.txt [22]
  http://ietf.org/rfc/rfc1035.txt [23]
- **BIND, a widely deployed nameserver product**
  http://www.isc.org/sw/bind/ [24]

Display as Single Column?:

The URIBL List in Janet

The URIBL List in Janet

The URIBL List in Janet

Janet has taken out subscriptions for the multi.uribl.com list on behalf of all Janet customer organisations. This allows Janet to replicate the list and make it available to all organisations on Janet.

The details of the multi.uribl.com list can be found at:

http://www.uribl.com [25]

How to use the Janet URIBL list

If your organisation has a Janet connection and wishes to use URIBL, you need only set the zone where the lookups are made, following the documentation for your e-mail server product, to:

multi.uribl.dnsbl.ja.net

gold.uribl.dnsbl.ja.net

black.uribl.dnsbl.ja.net

If your organisation uses the URIBL as part of an imported spam update, i.e. embedded in

spamassassin or some other antispam method with regular updates, you can access the mirrors under their original names but you will need to configure your nameserver to forward your queries for the zone to the Janet feed.

To access the Janet mirrors of URIBL as multi.uribl.com, you should put static forwarding in your nameservers to forward all queries for the lists to the Janet nameservers as detailed below:

ns0.mail-abuse.ja.net.	*128.86.8.120*
ns1.mail-abuse.ja.net.	*194.83.56.228*
ns2.mail-abuse.ja.net.	*194.83.56.244*
ns3.mail-abuse.ja.net.	*194.82.174.166*

The current list of nameservers can be obtained at any time by querying the addresses of ns.mail-abuse.ja.net. Janet will ensure that ns.mail-abuse.ja.net always has an up to date list of the nameservers serving the DNSBL mirrors it offers.

Conditions of use

Eligibility and charges

There is no charge to organisations with a Janet connection for use of the Janet URIBL feed.

URIBL reserves the right to restrict direct access to their nameservers. They may require heavy users to set up a transfer arrangement, for which their distribution contractors make a charge.

Access control

To ensure that Janet resources remain available to Janet organisations, the zones are served by dedicated nameservers, configured to respond only to queries which come from within Janet. Resolvers within Janet that have been seen to be using the lookup service are checked to ensure that they do not forward requests from outside Janet.

You MUST take whatever precautions are necessary to prevent access through your network from outside Janet.

Specifically, the DNS resolvers under your control MUST NOT accept recursive DNS queries from outside your own network for data in the zones within dnsbl.ja.net. Note that it is ordinary good practice to prevent all such recursive lookups from outside.

The Janet operators will record the IP address of each resolver (or perhaps e-mail server) making lookups from the zone, and will test it from time to time to confirm that it correctly rejects recursive queries.

• If it does indeed reject them, no action will be taken and it will be allowed to continue to lookup data from the zone.

• If it permits access which it should not, the Janet operators will attempt to contact the person

responsible for the IP address concerned, and will then help them to correct the faulty configuration. They may suggest workarounds if it proves difficult.

• If for any reason it is not possible to implement a secure arrangement within a reasonable period, the operators will bar access to the zones from the IP address concerned.

• If you believe you may have been barred, contact the Janet Service Desk [26].

Some networks may include DNS forwarders for internal use which are not themselves resolvers and are not the DNS clients known to the Janet nameservers. It is the responsibility of the organisation operating such a forwarder to ensure that it is not available for use from outside Janet; again, normal good practice is to make such a forwarder accessible only from within your own network.

Display as Single Column?:

DNSWL.org in Janet

DNSWL.org in Janet

DNSWL.org in Janet

Janet subscribes to a DNS allow lists with dnswl.org on behalf of the Janet community, and allows access to this allow lists to all organisations with a Janet connection.

The details of the allow lists can be found at:

http://www.dnswl.org/ [27]

How to use the Janet Allow lists

The allow lists are now available on the Janet DNSBL servers as:

- swl.dnsbl.ja.net (SpamHaus IP address allow lists)
- dwl.dnsbl.ja.net (SpamHaus Domain name allow lists) Please refer to http://www.spamhauswhitelist.com/en/ [28] for details.
- list.dnswl.dnsbl.ja.net (DNSWL IP address allow lists) Please refer to http://www.dnswl.org/tech [29] for details.

The lists are also available on our servers under their original names:-

- swl.spamhaus.org
- dwl.spamhaus.org
- list.dnswl.org

If you have externally updated software that uses the lists under their original names you can

still point the queries to the Janet servers, but you would need to configure your resolvers to forward the queries for these domains to our nameservers. If you need to do this, you MUST check periodically that the list of forwarders you are using is still correct.

To access the Janet mirrors of dnswl.org and/or SWL and DWL, you should put static forwarding in your nameservers to forward all queries for the lists to the Janet nameservers as detialed below:

- ns0.mail-abuse.ja.net. 128.86.8.120
- ns1.mail-abuse.ja.net. 194.83.56.228
- ns2.mail-abuse.ja.net. 194.83.56.244
- ns3.mail-abuse.ja.net. 194.82.174.166

The current list of nameservers can be obtained at any time by querying the addresses of ns.mail-abuse.ja.net. Janet will ensure that ns.mail-abuse.ja.net always has an up to date list of the nameservers serving the DNSWL mirrors it offers.

For sites using IPv6, you may also forward to the IPv6 addresses if preferred. Query ns.dnsbl.ja.net for AAAA records to get the list.

Conditions of Use

Eligibility and charges

There is no charge to orgainisations with with a Janet connection for the use of the Janet DNSWL.org, SWL and DWL feeds.

As part of our agreement with dnswl.org, we will process queries made to the DNSWL lists, and provide feedback on the addresses queried. The statistics provided will not contain any information about sites making queries to the zones, only the addresses looked up and the number of times each address was looked up will be reported.

Access control

To ensure that Janet resources remian available to Janet organisations, the zones are served by dedicated nameservers, configured to respond only to queries which come from within Janet.

The Janet DNSBL servers will not permit queries from open resolvers. If your resolver is open and allows general servers on the Internet to query records that you are not responsible for, your access will be blocked after a week or two, and will remain blocked until your server is secured. Some of the lists we serve require us to enforce this restriction to prevent their data leaking to people who are not authorised to receive it.

Display as Single Column?:

Links
[1] https://community.ja.net/library/janet-policies
[2] https://community.ja.net/library/janet-services-documentation/spamhaus-zen-lists-janet
[3] https://community.ja.net/library/janet-services-documentation/surbl-and-uribl-lists-janet
[4] https://community.ja.net/library/janet-services-documentation/dnswlorg-janet
[5] https://community.ja.net/library/janet-services-documentation/what-do-if-your-mail-being-blocked-0

[6] http://www.spamhaus.org/sbl/index.lasso
[7] mailto:help@jisc.ac.uk
[8] http://www.spamhaus.org/
[9] http://www.declude.com/Articles.asp?ID=97
[10] https://community.jisc.ac.uk/library/janet-services-documentation/what-do-if-your-mail-being-blocked-0
[11] http://support.microsoft.com/kb/823866
[12] http://www.exim.org/howto/rbl.html
[13] http://www.exim.org/exim-pdf-current/doc/spec.pdf
[14] http://www.postfix.org/
[15] http://qmail.virginmedia.com/top.html
[16] http://www.thedjbway.org/djbrbl/rblsmtpd.html
[17] http://www.sendmail.org/doc/
[18] http://spamassassin.apache.org/
[19] http://www.mailscanner.org.uk/
[20] http://ietf.org/rfc/rfc2821.txt
[21] http://ietf.org/rfc/rfc3463.txt
[22] http://ietf.org/rfc/rfc1034.txt
[23] http://ietf.org/rfc/rfc1035.txt
[24] http://www.isc.org/sw/bind/
[25] http://www.uribl.com
[26] mailto:help@jisc.ac.uk?subject=URIBL%20List
[27] http://www.dnswl.org/
[28] http://www.spamhauswhitelist.com/en/
[29] http://www.dnswl.org/tech