

JANET and Internet Filtering

1 Introduction

This document is intended to provide guidance for organisations connected to the JANET network on the subject of Internet content filtering. It outlines what filtering is performed by JANET and the approaches that can be taken by individual organisations to apply further constraints on the material accessible to their users. It also points to other sources of advice.

2 Background

The JANET network is an integral part of the global Internet, connecting together the LANs (Local Area Networks) of education and research organisations across the UK. With user organisations ranging from schools to advanced scientific research groups, the range of requirements of the network is very wide. The basic aim of JANET is, therefore, to provide a highly reliable, high-speed national network that enables customer organisations (individually or in groups) to build or obtain the particular combination of services they need.

As the JANET community has grown (particularly with the inclusion of under-18s from schools and colleges) and with growing concern about the availability of unsuitable content on the Internet, the issue of content filtering has become increasingly important. Even within an organisation, content filtering requirements will vary: material unsuitable for the younger pupils in a school may have educational value for their older peers. The approach taken by the JANET network allows organisations or sectors the flexibility to implement and manage appropriate content filtering for their particular requirements.

Whilst there are a number of technical solutions to the problems of blocking access to specific sites on the Internet and filtering inappropriate material on the basis of its content, it should be recognised that these tools, either singly or in combination, will not be 100% effective in restricting access to inappropriate material. In addition, some types of filter may also block legitimate material that is either similar to or located close to the offending material. It is therefore recommended that any technical solutions deployed at a given site should be supported by other measures, including education on how to avoid and deal with inappropriate material and the implementation and enforcement of an AUP (Acceptable Use Policy) governing network access and computer use.

3 Acceptable Use Policy

In common with many other network providers, JANET operates an AUP, which can be found at: <http://www.ja.net/services/publications/policy/aup.html>

It is a requirement for connection to the JANET network that each organisation agrees to comply with the JANET AUP. Having an AUP does not, and cannot, mean that non-compliant use will never occur. The purpose of the AUP is to ensure, as far as possible, that JANET services are used in an acceptable manner and in accordance with current legislation. Complying with the AUP also avoids the waste of resources, both for connected organisations and for the network, that is likely to be attendant on inappropriate or illegal usage. Connected organisations are expected to take reasonable measures to discourage behaviour that does not comply with the AUP and to take prompt and effective action to deal with complaints that the policy has been breached. The JANET AUP does not require organisations to make it impossible for their users to act other than in accordance with it.

Connected organisations are strongly recommended to incorporate at least the same principles into their own local AUPs, along with any further site-specific requirements. They must also ensure that individual users are aware of the JANET AUP and the fact that they are bound by it. The consequences of failure to comply with AUPs (which may include suspension or revocation of computer and network access) should be made clear to users in advance. For avoidance of doubt, it may be helpful to have users sign an agreement to this effect when they are first granted network access. Reminders of the applicable policies — for example, through signs or login boxes — are often useful in maintaining the level of compliance.

4 Why Filter?

Filtering is often used to protect the networks and computers of connected organisations from hostile or unwanted network traffic. This type of filtering could be based either on the source of the traffic (such as an external site known to be sending large volumes of unsolicited bulk e-mail) or on the destination (such as sensitive internal administration systems or subnets). Filtering unwanted large traffic flows can sometimes reduce network congestion, thus improving performance for priority applications, although this depends on the nature of the traffic and where it is blocked.

Filtering can also be used to force traffic to follow a particular route through the network. For example, an organisation may wish to implement a policy that all outgoing mail messages must go through an organisational mailserver, or that all web browsing must be done via the organisation's web proxy/cache. The former policy can both limit the spread of viruses and ensure that internal mail addresses are not revealed; the latter is essential to prevent users simply bypassing any content filtering performed by the proxy/cache.

Some organisations also now wish to use filtering to prevent their users from accessing illegal or inappropriate material. It may be more challenging to implement filtering for this purpose than for those listed above, as many of the sites that contain inappropriate or illegal material will also contain material that is harmless or even beneficial. Simply blocking access to the whole site will exclude all of its content. To avoid this, a filter is needed that can determine the particular part of the site (often represented by a URL) that is being requested and decide whether to block or permit access at this more specific level. As mentioned above, the definition of appropriate may also vary between groups of users, so the settings for this type of filter may need to change frequently as different groups use the same computers.

5 What Blocking or Filtering Does JANET Provide?

The JANET network is designed and operated so as to allow connected organisations as much flexibility as possible in determining their most appropriate network service. At the network level, therefore, blocking is only used when required by the JANET Security Policy as a limited short-term measure to protect a particular organisation or service from an imminent technical security risk until the organisation has been able to address the problem itself. Other than these temporary security measures, there is no centrally imposed filtering of web, e-mail or other content provided by the network; indeed, such filtering would be ineffective as the network provides many possible routes to bypass any solution implemented at a single point.

A number of the application-level services offered across JANET include filtering or blocking of some types of content, either as a permanent feature or as an option that can be enabled and configured by organisations using these services. These services are available to organisations with a Primary JANET connection.

- The **JANET Web Filtering Service** allows subscribing organisations to manage filters that will be applied to web requests made by users at the organisation. Filters are controlled through a web interface by authorised individuals at each organisation: rules can be based on individual URLs as well as pre-configured categories of material that may be inappropriate. The Web Filtering Service blocks access to URLs which are on the Internet Watch Foundation's list of content which is illegal under UK law.

Note: Like any filtering service, the filters will be ineffective unless the organisation configures its own browsers and web proxy to send requests to the Filtering Service, and its routers or firewalls to prevent attempts to circumvent the Filtering Service.

For more details see:

<http://www.ja.net/services/network-services/web-services/web-filtering/web-filtering.html>

- The **JANET Webmail Service**, designed for use by smaller organisations, includes options to filter incoming and outgoing mail against lists of inappropriate domains and words, as well as against viruses and spam. For more details see:
- Organisations running their own mail services can use the JANET subscription to the **Mail Abuse Prevention System** list of those Internet addresses which are associated with the sending of unsolicited bulk e-mail. Depending on their mail software, organisations can configure their systems to reject all mail from addresses on the list, or to require it to pass more stringent anti-spam tests before being accepted. For more details see:
- The **JANET Usenet News Services** exclude a number of specific newsgroups including those regarded by the Internet Watch Foundation as likely to contain illegal material. Organisations subscribing to these services can further restrict the newsgroups they wish their users to have access to. Messages likely to be spam, either because of their size or the number of groups to which they are posted, are also excluded. For further details, see:

6 Methods of Filtering Web Content

Since the JANET network does not contain built-in filtering of web or other content, connected organisations wishing to restrict access to specific material or sites on the Internet will need to implement or obtain mechanisms to do this. They will also need to configure their own network routers or firewalls to block or re-direct deliberate or accidental attempts to bypass their filters. Filters that are managed by individual organisations (whether implemented at the organisation or elsewhere) and supported by local network and system configuration are both the most effective and least disruptive way to enforce the policy of the individual organisation.

Provided the local network is properly configured, the openness of the JANET network means that the filtering system can be equally effective wherever it is physically located. Appropriate filtering solutions may be available from local consortia, from UKERNA (as described above) or from national providers. Two approaches to filtering, which may be used in combination, are in common use:

6.1 Packet filtering

Typically implemented on routers, the source addresses and port numbers of individual incoming IP packets are examined and compared against a banned list, and packets are only transmitted if there is no match. This approach results in blocking all traffic to or from the specific sites or networks in the banned list, or using a specified port number (which may correspond to a type of network service), whether the actual traffic is wanted or unwanted. The effort required to maintain the list of banned sites means that this approach is suitable only for fairly static lists.

6.2 Application content filtering

This requires all off-site traffic to be routed through a proxy server which retrieves web pages on behalf of the requesting client system. The proxy server system runs software that can simply be configured to block access to entire sites based upon lists of banned addresses, as for packet filtering. However, proxy servers can also block access to specific web pages within a site by checking the web page address (or URL) or in some cases by examining the content of a requested page for specific keywords. This type of filtering can be more precise in the rules it applies, particularly where large websites contain only a minority of inappropriate material.

There are many commercial packages available which provide content filtering functionality, with regularly updated lists of banned sites that may be rated by category, age, or other factors. Reviews of a number of these packages are available through some of the web references given at the end of this document. The Squid project also offers a freeware package, available for Linux®/UNIX® and Windows NT® systems. It should be noted that JANET does not recommend specific content filtering software.

These techniques are not and cannot be completely reliable for preventing deliberate or accidental access to inappropriate material. Lists of banned sites require regular maintenance, and so will not always be up to date. Additionally, there are well-known methods for evading the checks (e.g. the use of translation engines, or the embedding of redundant username and password information in URLs). A further important consideration in the deployment of a proxy server is that it can introduce a potential point of failure into an organisation's network infrastructure. If all network access is directed through a proxy server, then failure of that system can result in no Internet access from client systems. Inadequate proxy server hardware can also result in (apparently) degraded network performance for users.

7 A Complementary Approach

It is suggested that organisations concerned about blocking access to Internet content should adopt a multi-faceted approach to the problem, combining administrative, educational and technical elements. They should:

- Agree a policy about what Internet content is suitable and what is unsuitable.
- Publicise that policy and incorporate its aims into an AUP.
- Ensure that all staff, students and visitors agree to comply with the AUP when first granted computer and network access, and make clear what the penalties are for non-compliance.
- Educate users in how to deal with inappropriate material they may find: in particular, encouraging them to report, rather than conceal, any accidental discovery of unsuitable material.
- Locate public access computers in open, supervised areas; if appropriate, requiring Internet use to be accompanied or supervised.
- Implement technical measures where appropriate (for example, a proxy server) to enforce the policy on acceptable use. Such measures must be accompanied by appropriate configuration of the local network routers or firewalls, or they will be ineffective.
- Use the monitoring capabilities of content blocking software to log network activity, and review the logs on a regular basis. Such monitoring must comply with the Data Protection Act 1998 and Regulation of Investigatory Powers Act 2000 and in particular, users must be informed that their use will be monitored.
- Take appropriate action against any instances of non-compliance with the AUP.

8 Suggested Web Sites for Further Information

- <http://schools.becta.org.uk/index.php?section=is>
Becta e-Safety site, covering safe use of the Internet.
- <http://www.iwf.org.uk/>
Home page for the Internet Watch Foundation, a UK body concerned with the issue of illegal material on the Internet.
- <http://www.more.net/technical/netserv/tcpip/ipfiltering.html>
Missouri Research and Education Network report on filtering.
- <http://aocnilta.co.uk/2006/08/03/dopa/>
AoC NILTA paper on filtering versus education.
- <http://www.squid-cache.org/>
Home page for the Squid web proxy cache software, including download information, configuration guide and user documentation.