



Guidance Notes

JANET and Internet Filtering

**Stephen Percival
UKERNA**

GD/NOTE/006

JANET Guidance Notes

JANET Guidance Notes are one of a series of user guides available to JANET customers. Guidance Notes do not generally contain detailed technical information and are primarily aimed at customers who wish to extend their general knowledge of a particular subject. These guides provide readers with a wide variety of general information, case studies and advice.

If you have any queries or comments about the Guidance Notes or would like to obtain copies, please contact:

JANET Customer Service

UKERNA

Atlas Centre, Chilton, Didcot

Oxfordshire, OX11 0QS

Tel: 01235 822212

Fax: 01235 822397

E-mail: service@ukerna.ac.uk

Further details of the documents in this series are available at:

<http://www.ja.net/documents/index.html>

Contents

- 1 Introduction
- 2 Background
- 3 Acceptable Use Policy
- 4 Why filter?
- 5 What blocking or filtering does JANET provide?
- 6 Methods of filtering web content
- 7 Complementary approach
- 8 Suggested web sites for further information

1 Introduction

This document is intended to provide guidance on the subject of Internet content filtering for organisations newly connected to the JANET network. It outlines what filtering is performed by JANET, and the approaches that can be taken to apply further constraints on what material is accessible from a JANET connected site, and provides pointers to other sources of advice.

2 Background

The JANET network is an integral part of the global Internet. It has for some years connected all of the UK Higher Education Institutions and Research Councils, and more recently has been extended to the colleges of Further Education in the Learning and Skills sector. With the extension of the JANET user base to under-18s (principally in FE colleges) and growing concerns over access to illegal or inappropriate content on the Internet, especially by minors, the issue of content filtering has become increasingly important.

Whilst there are a number of technical solutions to the problem of blocking access to specific sites on the Internet and to 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. It is therefore recommended that any such solutions deployed at a given site should be supported by other measures, such as the implementation and enforcement of an Acceptable Use Policy (AUP) governing network access and computer use.

3 Acceptable Use Policy

JANET, in common with many other network providers, operates an AUP which can be found at:

http://www.ja.net/documents/use_policy.pdf

It is intended to prohibit illegal and inappropriate use of the network, and to prevent the consequent waste of resources attendant on such usage.

It is a requirement for connection to the network that an organisation agrees to comply with the JANET AUP. Connected organisations are strongly recommended to incorporate the same principles into their own AUP, along with any further site specific requirements that they may have. They must also ensure that individual users sign an agreement requiring their conformance to the AUP, when first granted network access. The consequences of failure to comply with the AUP, which may include suspension or revocation of computer and network access, should be made clear to users in advance.

4 Why filter?

The principal reason for filtering is to prevent access to illegal or inappropriate material. Implementing filtering may also have the beneficial side effect of reducing traffic on the JANET connection to a site, thus improving access for appropriate uses of the network.

5 What blocking or filtering does JANET provide?

JANET's connectivity to the US Internet is filtered to the extent that all traffic is blocked to networks listed on the Realtime Blackhole List (RBL). For further details, see:

<http://www.ja.net/CERT/JANET-CERT/mail/junk/teleglobe-rbl.html>

The primary reason for this restriction is to block access to networks known to be originators of unsolicited e-mail, but the effect is to prohibit all traffic to and from the listed networks.

Additionally, filtering is performed on the JANET Usenet News feed, with a number of specific newsgroups excluded from the feed supplied by JANET. The list of excluded newsgroups is available at:

<http://www.ja.net/usenet/banlist.html>

Organisations subscribing to the News Reader or News Cache services may elect to further restrict the Newsgroups available to users at their sites, in accordance with the documentation for configuration of these services.

There is no central filtering of web content or e-mail carried across the JANET network (beyond that resulting from subscription to the RBL).

6 Methods of filtering web content

Since JANET does not centrally filter web content, connected organisations that wish to restrict access to specific material or sites on the Internet will need to implement mechanisms to achieve this. There are two approaches in common use:

- **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 of particular types of traffic (where this is associated with a specific port number). The effort required to maintain the list of banned sites means that this approach is suitable only for fairly static lists.
- **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 block access to entire sites based upon lists of banned addresses, as for packet filtering. Proxy servers can also block access to specific web pages within a site by checking the web page address (or Uniform Resource Locator, URL) or in some cases by examining the content of a requested page for specific keywords. There are many commercial packages available providing content filtering functionality, with regularly updated lists of banned sites. 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 UKERNA does not recommend specific content filtering software.

These techniques are not and cannot be completely reliable for preventing 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 another 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 Complementary approach

It is suggested that organisations concerned about blocking access to Internet content should adopt a multi-faceted approach to the problem, combining both technical and administrative 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 sign an agreement to comply with the AUP when first granted computer and network access, and make clear what the penalties are for non-compliance;
- locate public access computers in open, supervised areas;
- implement technical measures where appropriate (e.g. a proxy server) to enforce the policy on acceptable use;
- use the monitoring capabilities of content blocking software to log network activity, and review the logs on a regular basis;
- take appropriate action against any instances of non-compliance with the AUP.

8 Suggested web sites for further information

<http://safety.ngfl.gov.uk/>

National Grid for Learning site, covering safe use of the Internet.

<http://www.iwf.org.uk/>

Home page for the Internet Watch Foundation, a UK based body concerned with the issue of illegal material on the Internet.

<http://www.more.net/rnd/ipfiltering.html>

Missouri Research and Education Network report on filtering.

http://www.noie.gov.au/projects/consumer/content_regulation/blocking1/blocking.htm

Comprehensive technical report on Internet content blocking, prepared for the (Australian) National Office for the Information Economy.

<http://www.rsc-london.ac.uk/networking/filter.htm>

JISC Regional Support Centre for London review of technical aspects of packet and content filtering.

<http://www.squid-cache.org/>

Home page for the Squid web proxy cache software, including download information, configuration guide and user documentation.

Tell us what you think

Guidance Notes are produced and published by UKERNA for use within the JANET Community. We welcome your comments on all aspects of this document and on any other UKERNA publication. Please direct feedback to JANET Customer Service, at the address below, or e-mail us directly at:

documentation@ukerna.ac.uk

UKERNA manages the networking programme on behalf of the higher and further education and research community in the United Kingdom. JANET, the United Kingdom's academic and research network, is funded by the Joint Information Systems Committee (JISC).

For further information please contact:

JANET Customer Service
UKERNA
Atlas Centre, Chilton, Didcot
Oxfordshire, OX11 0QS

Tel: +44 (0) 1235 822 212
Fax: +44 (0) 1235 822 397
E-mail: service@ukerna.ac.uk

Copyright:

This document is copyright The JNT Association trading as UKERNA. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from JANET Customer Service.

Trademarks:

JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.

Disclaimer:

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution.

The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

Availability:

Further copies of this document may be obtained from JANET Customer Service at the above address.

This document is also available electronically from: http://www.ja.net/documents/gn_filter.pdf



© The JNT Association 2001

**Joint Information
Systems Committee**