

23

Open Source, DansGuardian 2.9

DansGuardian is an open source web content filter available on Linux and MacOS.

Its support of platforms and languages is summarised in the table below:

Type	Client	Server	Service						
Platforms	Win95	Win98	WinME	Win2k	Win03	WinNT	WinXP	Linux	MacOS
Protocols / Applications	browser	instant msg	chat	e-mail	news	file transfer	peer2peer	VoIP	Stream
Languages User Interface	Czech	Danish	Dutch	English	Estonian	Finnish	French	German	Greek
	Polish	Portuguese	Slovak	Slovenian	Spanish	Swedish	Maltese		
Languages Filtering Criteria	Czech	Danish	Dutch	English	Estonian	Finnish	French	German	Greek
	Polish	Portuguese	Slovak	Slovenian	Spanish	Swedish	Maltese		

The feedback given by the User Reference Group is summarised as follows:

Test domain	Score	Actual score	Average all tools	Best tool
(Un)installing and updating the tool	●○○○	1,8	2,3	2,8
Tailoring and monitoring the filtering	●●○○	2,4	2,5	3,2

The scores of the Lab tests are summarised as follows:

Test domain	Score	Actual score	Average all tools	Best tool
Local language support	●●○○	2,0	2,6	4,0
Effectiveness for kids	●●○○	2,5	2,0	4,0
Effectiveness for adolescents	●●○○	2,5	1,8	2,5
Effectiveness for kids (porn only)	●●●○	3,0	2,6	4,0
Effectiveness for adolescents (porn only)	●●●○	3,5	2,5	4,0
Speed of filtering	●●●○	3,0	3,2	4,0
Security Integrity	●●●○	3,0	2,7	4,0
Legal Compliance	●○○○	1,0	2,4	3,5

1. Configurability

Installation of DansGuardian demands some knowledge on how to compile and how to install software in a Linux environment. DansGuardian needs an upstream proxy-server to operate effectively. DansGuardian can be easily integrated in a network where a proxy server is already active. The network where DansGuardian is installed should automatically redirect all web requests to the DansGuardian module (a transparent proxy setup) or all clients should be individually set up to use the DansGuardian module.

The tool comes with a very useful default filtering policy, which is however rather difficult to fine-tune.

Several harmful content categories are available and the child carer can easily add specific websites to the black and white list.

It is possible to link the filtering functionalities to different users or groups of users.

DansGuardian can only be updated manually, for all PCs simultaneously.

2. Usability

DansGuardian does not have a user friendly interface. Configuration options are only accessible via different configuration files (text). Some configuration options may be difficult to understand for non-technical users. Help information is available and easily accessible.

The manuals require also some technical knowledge.

3. Filtering Algorithm & Effectiveness

The scores of the Lab tests for the individual effectiveness tests are:

Content Type	Score
Web ICRA filtering	4
Instant Messaging	N/A
Chat	N/A
Email	N/A
Newsgroup	N/A
File Transfer Protocol	N/A
Voice over IP	N/A
Streaming media	N/A
Peer-to-peer	N/A

Web filtering: URL based filtering

In addition to the URL black list used by the filtering tool, the child carer can add website URLs to a custom black list.

Web filtering: Content filtering

When a website contains too much harmful phrases or keywords, the website is blocked. The tool takes ICRA labels into account.

Instant messaging MSN

The tool does not allow child carers to block instant messaging applications.

Chat IRC filtering

The tool does not provide the option to filter or block IRC applications.

Email filtering

The tool does not provide the option to filter or block email applications.

Newsgroup filtering

The tool does not provide the option to filter or block newsgroup applications. Messages could be downloaded and were not filtered.

File Transfer (FTP) filtering

The tool does not provide the option to filter or block FTP applications.

Voice over IP, streaming media, peer-to-peer blocking

The tool does not provide the option to filter or block VoIP.

The tool does not provide the option to filter or block streaming media.

The tool does not provide the option to filter or block peer-to-peer blocking.

4. Performance

The CPU and memory consumption tests are only applicable to end users systems and were not performed on the servers.

Based on the HTTP loading tests for this tool, it scored a 3, meaning that there was a low impact in terms of delays and therefore did not degrade the surfing experience significantly.

5. Transparency

When logging in, the user is not informed of any logging, monitoring or filtering activities.

When the user tries to open a prohibited website, a notification is given that the content is blocked. This warning message can be adjusted by changing the source files and it is not possible to overrule the blocked function. The message also contains the reason (content category) why the website has been blocked.

Summarised and more detailed reports are available in the form of log files on the server on which DansGuardian has been installed.

6. Security Integrity

Network tests

The results of the network scans showed that the setup of the DansGuardian proxy service was not secure. We could identify weaknesses with default configuration options, the risk of cross-site scripting, unsafe options supported, etc.

Local tests

Since the product is server based, children do not have access to the server, but only to its filtering services. Therefore, many of the local tests done with client side tools were not applicable to server based solutions. We did not identify security issues during the local tests.

7. Legal Compliance

The DansGuardian product is offered for free to non-commercial users under an open-source license (GPL). Users are clearly informed about the limitations of use and conditions of downloading the product. These limitations are actually in line with the principles and limitations governing the use and roll-out of open source solutions. However, except these license terms, no other legal information is conveyed on the vendor's website, neither a privacy statement.

If the absence of more detailed legal rules is justified by the fact that the product is open source, offered for free and without further warranties of use (being normal for open source), more attention should be paid to the privacy statement. The only phrase we currently found on the product's website is that email addresses of people visiting the website are never passed on to third parties. However, a number of other personal information is required while users register on-line (optional).