



Streamlining Internet policies

Get the full picture and gain control of your network

Danware Data A/S
Bregnerodvej 127
3460 Birkerød
Denmark
Tel.: +45 45 90 25 25
Fax.: +45 45 90 25 26
www.netop.com

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

Abstract

In some cases users of Internet, chat and peer-to-peer pose no threat to an organization. In some cases management gets a rude awakening: Productivity may decline, costs may rise significantly, slow Internet connections and, finally, music, films – protected by copyright legislation – and pornography may be saved on the organization's servers causing legal action against the organization.

These challenges are real and omnipresent.

There is a growing awareness about these problems – but how can an organization deal with it? Shutting down the Internet connection? A written policy in the employee handbook? Neither solution is practical.

Active filtering is.

The simple way to start filtering is to install Eclient on all user computers and NetOp Netfilter on a server and direct all Internet traffic through it.

The solution

NetOp Netfilter offers a simple, yet powerful solution to the problems described above.

NetOp Netfilter offers a wide selection of filtering and blocking tools, all of which can be set up easily. The focus of this whitepaper is chat and peer-to-peer.

To block chat and peer-to-peer a client-server system must be set up. The system consists of a server running NetOp Netfilter and a client running NetOp Eclient.

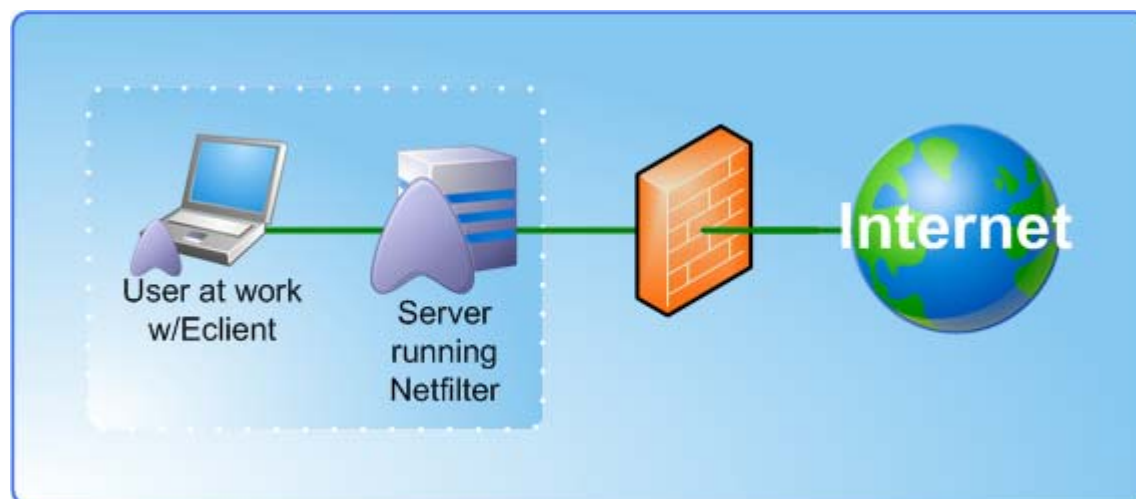


Figure 1: Typical scenario. Organization network computers running Eclient connect to the Internet through a server running NetOp Netfilter.

While the client is on the organization's network it will be subjected to the rules set up on the NetOp Netfilter – when the user takes the laptop home, the “filter is off”.

The NetOp Netfilter is an administrative tool with numerous functions. It must be installed on the server which routes all Internet traffic.

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

The NetOp Eclient is a small Windows executable that can be run on the client computers offering two key functions. Firstly, it can work as a sender/receiver that exchanges information with the Netfilter block/allow lists which programs should be DISallowed on the client's computer. Secondly, if logging by username is required then Eclient must be used.

The administration module offers intuitive tools to adjust the filter to the organization's requirements. To filter and log the traffic – both amount of downloaded megabytes and visited Internet sites – set the appropriate checkmarks in the Admin-module.

The log file will provide the full picture of the organization's bandwidth consumption and visited web sites.

Initially, chat and peer-to-peer are allowed (as are many other actions). To block e.g. chat, open the administration application and select which chat programs should be blocked.

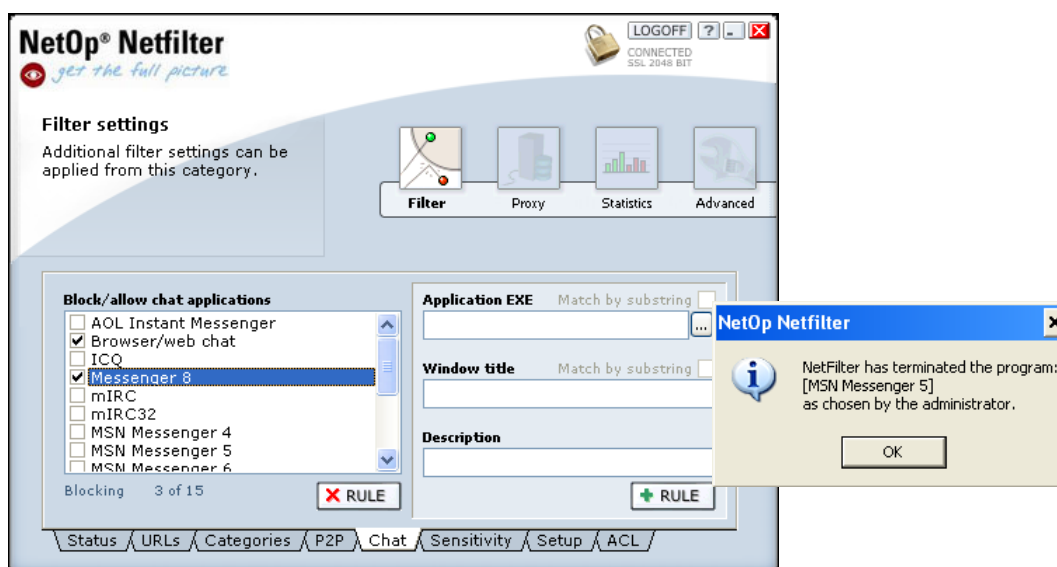


Figure 2: Administrator's module and the resulting message on the client's screen.

Be aware that some people in your organization may use chat as part of their job. See "Who'll see what?" to learn about differentiated filtering.

The administrator can block media types, peer-to-peer, chat etc. The user will be notified by a sign when he tries to access or use these.

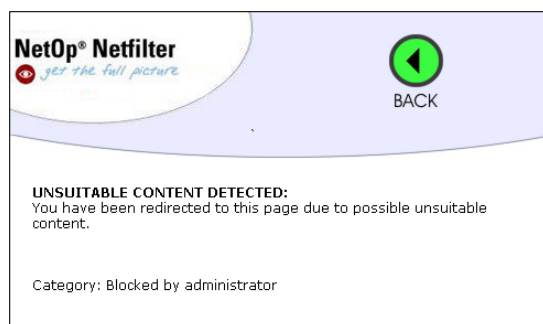


Figure 3: NetOp Netfilter, action blocked by administrator.

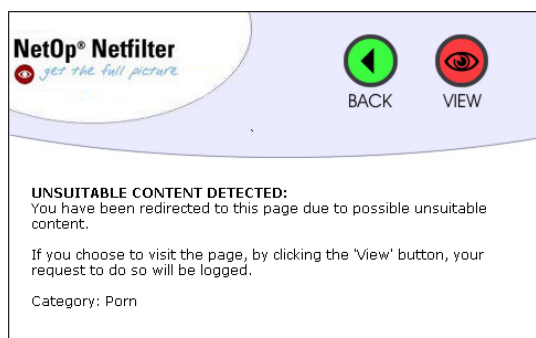


Figure 4: NetOp Netfilter, category filtering.

Apart from the block, which effectively limits the users' possibilities of certain tasks, NetOp Netfilter also offers a state of the art adaptive filtering. The filtering is split into five categories: Pornography, hate, violence, illegal activities and copyright violation.

The administrator can select to allow users to continue after the warning sign is displayed. As a user you are allowed to continue, but you are warned that your activities are logged.

The administrator can remove the possibility to 'View' a web site considered to be in violation of the category rules.

A combination of NetOp Netfilter and an outspoken company policy just may spare your company from negative media coverage.

Note: Please check with local legislation before starting to log user behavior.

Note: Companies may be held liable even though it is the employees which violate copyright legislation or child pornography legislation.

Who'll see what?

NetOp Netfilter can grant some users access to certain file types or Internet sites, while other users are blocked from the same content.

Grouping users in different segments allow the organization to 'tighten the leash' on one group of users while another group can be granted a higher degree of freedom.

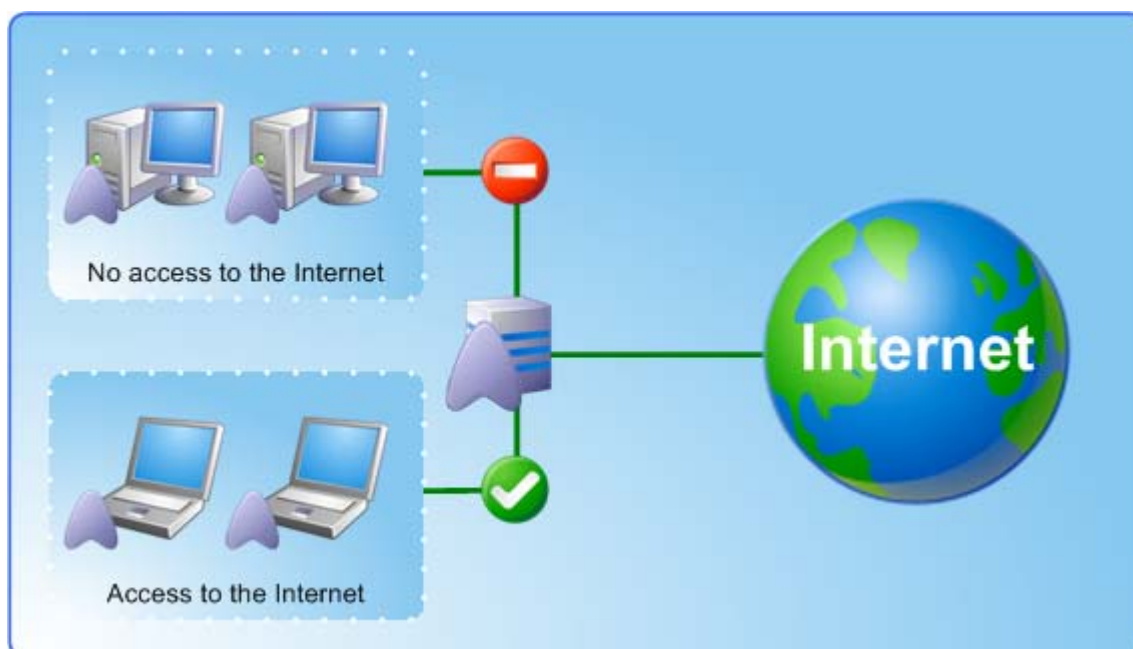


Fig. 5: Different policies for different groups within the organization: Some users have access to the internet while others don't.

Users can be divided into groups or segments to tailor the filtering to the organization's needs and preferences.

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.



Benefits

To run an organization the administration has to examine the threats.

The unique construction of NetOp Netfilter combines adaptive filtering with static lists of unwanted URLs. Most Internet sites which have questionable content will be caught by one of the three 'automatic' filters (Categories, Chat and P2P), but some sites are just unwanted. Add these sites to the 'Always block list'.

Note: There is an 'Always grant list' as well.

Single point of communication targets all PCs of the organization: Make all PCs access the Internet through the same port – and all actions that resulted in the 'User warning' (Figure 4) screen will be logged.

Target Industries

Schools, High schools, and Universities, Municipal and governmental offices or privately held companies

Questions and Answers

Will NetOp Netfilter block all explicit content?

No, it will block most pornographic content, which has sexually oriented text and color photos; if the text is neutral and the images either drawn or in black/white, the page will pass.

Will NetOp Netfilter slow down the Internet?

No. The NetOp Netfilter does not use the available bandwidth. It may slow down the perceived speed because the content has to be scanned before it is displayed.

Do you have to install NetOp Netfilter on all the organization's PCs?

No. Once the NetOp Netfilter is installed on the server and the users are routed through the designated port, Internet filtering is active.

Can users have different profiles?

Yes. NetOp Netfilter can divide users into groups with different rights. The division into segments is based on e.g. the users' DNS names, user names, Active Directory or their IP addresses.

The list of chat programs does not cover all. Can I add programs?

Yes! On the right side of the chat-tab you can enter the description and the executable's name and add it to the list. The same applies to peer-to-peer programs. See figure 2.

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

NetOp® Netfilter



Will my computer be protected from virus, worms etc.?

No. NetOp Netfilter does not protect against malicious software. It may, however, prevent users from inadvertently to let virus into their computers because they are stopped before entering questionable sites.

What is the problem with users chatting and downloading?

The problem is two-sided: Firstly, the user is not being productive and, secondly, risk of virus.

Who is Danware?

Danware's core business is to develop and market software products based on the NetOp core technology – a technology enabling swift, secure and seamless transfer of screens, sound and data between two or more computers.

The organization's three product areas are Desktop Management, Education and Security. The core Desktop Management product, NetOp Remote Control, enables remote control of one or more computers from another computer and can be used across different system platforms. NetOp School, the Education core product, is a software application for computer-based classroom teaching in both physical and virtual classrooms via the Internet or other networks. The Security business products are NetOp Desktop Firewall and NetOp Netfilter. All are plug 'n play products offering extensive functionality, flexibility and user-friendliness.

See more at: <http://www.netop.com/netop-471.htm>