

NetOp[®] Netfilter

get the full picture



Protecting company assets

Product White Paper



Protecting company assets

In many cases the fact that employees within a company have unrestricted access to the Internet as well as chat and peer-to-peer programs does not constitute a problem.

In other case scenarios a company may suffer deeply from the lack of control: productivity decline, significant cost increase and unnecessarily slow Internet connections. Also, a company might have to face legal actions as a consequence of illegal or inappropriate download and storage of files on corporate servers. Additionally, the company might risk exposing invaluable intellectual property.

Such risks are very real and could potentially damage any organization.

Awareness about these issues is growing but what practical measures does an organization have for dealing with them? Closing down employees' Internet access? Updating the employee handbook with Internet access guidelines? Hardly practical alternatives in the real world!

Using effective software to protect company assets is! NetOp Netfilter offers a wide range of easy-to-set-up filtering and blocking mechanisms. NetOp Netfilter can help companies raise productivity, provide data leakage protection, and help keep networks free from attacks by worms, viruses, Trojans horses, malwares and spywares.

Surveys indicate that 12% of employees have, by accident or purposely, visited porn sites.

Maximize working hours

Surveys¹ of Internet and application usage in the workplace indicate that employees spend between 3 to 6 hours per week on non-business-related Web sites. This includes activities like surfing, shopping, pc-banking, downloading and chatting. This means that in a company with 100 employees, 300 to 600 hours corresponding to full working hours of 7 to 15 employees. So limiting access to some of these non-business-related Web sites would free up substantial resources and thus enable the company to maximize use of working hours.

It is also important, though, that Internet solutions balance employees' needs for personal use of the Web at work without draining overall productivity or morale, all the while keeping employees safe from Web-based security threats.

NetOp Netfilter's customizable blacklists and built-in filtering categories are efficient options that can completely block access to specific sites, or filter on certain content types like gambling or dating.

Surveys indicate that 24% of employees watch or listen to streaming media at least once a week.

Use bandwidth effectively

Although non-business-related Internet use may constitute less than approximately 10% of the working hours, the corresponding bandwidth load is often dramatically higher. This is due to the fact that non-business-related Internet

¹ See for example reports on www.harrisinteractive.com

use frequently involves downloading, streaming and pictures. When network bandwidth is used for other than business tasks, less bandwidth is available for legitimate business activities. This in turn may lead to reduced employee efficiency.

Making sure that employees do not – whether purposely or inadvertently - access bandwidth-intensive sites, means faster access and higher efficiency for the business. NetOp Netfilter's blacklists and categories can also make a difference here.

The business network is also impacted by the download of large files and while some such file downloads may be required for business purposes, other downloads may just be 'noise'. NetOp Netfilter can be set up to detect and block MP3 transfers by binary analysis. This means that even MP3 files that have another file extension are identified for what they are. NetOp Netfilter can also be set up to generally detect and block download of large files where 'large' is completely configurable size.

Surveys indicate that 18% of employees download MP3 files or other non-business-related files - and that these files take up an estimated 7.5% of the total disk space.

Protect against malware

Employees' use of bandwidth-intensive, non-business-related Internet sites is not only a matter of productivity and efficient use of available resources. The hidden software on some of these Web sites also poses a substantial threat: Employees may unwittingly download virus, malicious software or other malware that could infect the entire company network – one accidental click of the mouse can take an entire network down for days at a time.

Because of the potentially disastrous consequences to business it makes perfect sense to install filtering technologies to manage which types of Web sites employees visit. Frequently sites visited by a large number of users are the sites that are targets by hackers. NetOp Netfilter's customizable blacklists and built-in filtering categories are efficient protection options that are easy to set up.

Secure sensitive information

Another unpleasant aspect of malicious software is the fact that its sole goal might well be to access sensitive or confidential information. As mentioned above, this is where NetOp Netfilter's blacklists and filtering categories can help protect employees from accessing Web-sites that are not related to the business.

Instant Messaging can potentially be dangerous because of the inherent element of trust: the users on your contact list are people you know! But like e-mail addresses, a contact list can be misused and a seemingly innocent link may have fatal consequence for the company network.

Sensitive information or intellectual property can also inadvertently be exposed through the use of peer-to-peer programs where the intent may be to share innocuous data like for example music files. NetOp Netfilter includes features to block the use of a long list of well-known peer-to-peer programs as well as the option to include other peer-to-peer programs to the default list.

Exposure – as well as injection of malware to the company network – may also occur through the use of chat program. NetOp Netfilter also includes features to block the use of a long list of well-known chat programs as well as the option to include other chat programs to the default list.

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 manufacturers. 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.

Ensure that copyright legislation is upheld

In addition to inefficient use of company assets and resources when downloading and storing files that are unrelated to the business, storage might also simply be a violation of the copyright legislation. Companies can be held responsible for any software, films or music files that are stored on company computers so it is in the interest of any company to ensure that pirated software, movies or music files are not available on company assets.

NetOp Netfilter's blocking of MP3 files as well as blocking for download of large files is a good way to help keep the company on the right side of the copyright legislation.

Summary

Below table summarizes the above-mentioned security goals and the NetOp Netfilter feature that can help achieve those goals.

Feature→ Goal↓	Categories	Block lists	Peer-to-peer	Chat	Large files	MP3 files
Maximize working hours	√	√				√
Use bandwidth effectively	√	√	√		√	√
Protect against malware	√	√				
Secure sensitive information			√	√		
Ensure that copyright legislation is upheld			√		√	√

Who is Danware?

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

The company has two product lines, Desktop Management and Education. The core Desktop Management product, NetOp® Remote Control, enables remote control of one or more computers. NetOp® School, the core Education product, is a software solution for computer-based classroom teaching. All are Plug and Play products with extensive functionality, flexibility and user-friendliness.

Danware's products are sold in more than 80 countries, and in 2006 the turnover was approximately EUR 12.9 million. Danware's shares are listed on the Copenhagen Stock Exchange (name DANW) and are part of the SmallCap+ index. Danware has subsidiaries in the U.S.A., the UK, and Germany. For further information, please see www.danware.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 manufacturers. 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.