

# NetOp<sup>®</sup> Netfilter

Datasheet, Business • 1/2

get the full picture



Protect your company. Let your employees browse the internet knowing that your IT policies are implemented – inside as well as outside the company network.

## The challenge for businesses

Unwanted web surfing hurts more than just your company's bandwidth. Illegal or copyrighted files and offensive materials can hurt your corporate image, offend other employees and pose a legal or financial liability to your company. In the worst case, the CEO is at risk of jail time. The other main reason for installing this technology is to tighten security by not allowing employees to go to unknown sites that could contain adware, spyware, Trojans or other kinds of malware which can compromise network security. Companies don't have the time or the staff to monitor all sites their users go to. Nor can they block sites that may be useful to certain departments and not others. Blocking certain categories has helped companies tremendously but some people still can find ways around it.

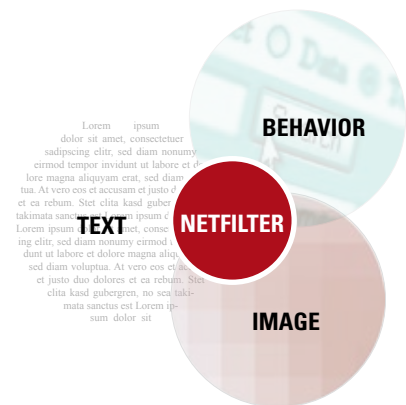
- Employees browse various non business related sites and download illegal or copyrighted files and offensive materials like pornography. Approximately 5% of all employees browse for pornographic material and some also for child pornography. If discovered, this can have a negative impact on the company reputation, a financial impact, and in worst case the CEO is at risk of jail time.
- Websites that seem safe may not be, and it is not unusual that these sites download malware to the endpoint without the user knowing about it. The company network will be infected and this can lead to data corruption or data leakage.
- Private surfing puts load on the bandwidth and that may impact performance for the effective employees since their access to business information will be slowed down.

Many companies have a conventional content filtering solution, which is based on URL blacklisting (fixed list of blocked URL addresses) or simple text analysis. Often they fall short and are too restrictive or too lenient, and they are not up to date. They are dependent on hourly updates since more than 1000 new URLs are created every minute. This is the reason why a blacklist will always be lacking. Also many companies are not protecting their laptops when they are outside the company network. Normally, laptops bypass any perimeter protection when an employee comes back into the office after traveling. When the laptops connect to the company network, they spread the malware.

## The NetOp solution

With NetOp Netfilter you get an intelligent filtering solution that is not dependant on constant updates.

NetOp Netfilter uses a unique filtering logarithm. It is a 100% real-time dynamic content filtering solution that is based on artificial intelligence. This solution combines advanced image, text, and behavior analysis and it is the necessary tool to guide your employees and prevent problematic web behavior. With NetOp Netfilter, you can make sure that any formulated policy can be implemented and enforced. This is done proactively, discreetly and automatically.



## At a Glance

- Manage and enforce your IT policy rules for Internet behavior easily and automatically
- Fast real-time, dynamic, and intelligent image analysis based on artificial intelligence
- 2 fold text analysis that evaluates the overall text on a site and not just words
- Personal behavior analysis that gives credit to those not violating internet policies
- Stop IM, P2P, streaming audio, and video, chat programs and any other program
- Import of blacklists
- No constant updates required
- Centrally managed
- Monitor individual behavior
- Reporting tool - easily drill down in detailed with statistics via the analysis tools
- Override functionality to give the users the benefit of the doubt by getting a warning, rather than simply being blocked
- The technology is build so it can grow with your business
- The image analysis checks all images for pornography or pornography related material (this covers also child pornography)

## Functions & advantages in detail

**Reliable, continually updated content filter** - NetOp Netfilter pursues a 100% dynamic approach and so is not dependent on URL lists that quickly become obsolete, unlike many other solutions. This means that even new websites can always be reliably analyzed and filtered in real time without any updating.

**Simple blocking of unwanted web content** - Block websites with the following content easily at the click of a mouse using built-in content categories: pornography, hate, racism & discrimination, violence & vulgar humor, copyright violations, illegal or dangerous activities, dating and gambling. You can also create your own categories based on URL lists.

**Outstanding filter accuracy** - Reliably identify unwanted content through a combination of leading technologies for professional text and image analysis and intelligent analysis of surfing behavior.

**Custom configuration options** - Adapt the software flexibly using configurable filter sensitivity, white lists, access control lists and time-specific filter settings.

**Blocking of chat and file-sharing programs** - Use the Netfilter client modules to suppress the execution of any chat and file-sharing programs centrally at the click of a mouse.

**Blocking unwanted file types** - Prevent the downloading of certain files or file types simply by specifying the file extension (e.g. '.divx', '.exe') or fragments of the file name. Reliably block MP3 files even if the file extension is deliberately modified, by analyzing the file header. Limit the network load by blocking streaming media and files above a certain size.

**Easy integration of laptops and home workstations** - Integrate computers outside the network fully and securely and administer them centrally using the free Business Desktop module.

**Virtually maintenance-free operation** - Use the dynamic, self-teaching filter technology and automated program updates to reduce required maintenance to a minimum.

**Comprehensive logging and statistics** - Log all activities and events centrally, down to user level if necessary, and view them graphically at any time. Integrate PCs outside the network using the free Business Desktop module.

**Efficient administration** - Use the intuitively operated Netfilter Admin management console to perform all configuration and maintenance tasks and view reports and logs remotely, saving you time. The flexible user management allows you to create multiple administrator accounts with different rights.

**High scalability** - Adapt the program to any network size using multiple centrally administered Netfilter installations.

## Modules

Netfilter Proxy Server	Central server module for filtering web content
Netfilter Admin	Console for (remote) administration and configuration
eClient Module (optional)	Add-on module for desktop PCs. Allows you to block chat and P2P file-sharing programs and log user names.
Business Desktop (optional)	Extended eClient module for mobile PCs & home workstations.
MySQL database (optional)	Database for extended logging and reporting. Required if using the Business Desktop module.

## System requirements

Netfilter Proxy Server	Windows NT/2000/2003 /2008 (incl. all server editions)
Netfilter Admin	Windows NT/2000/2003/2008/XP/Vista
Client PCs	All operating systems (Windows, Mac, Linux ...), Internetbrowsers with configurable proxy settings
eClient module	Windows 9x/Me/2000/XP/Vista
Business Desktop	Windows 2000/XP/Vista, requires Netfilter with MySQL

## Licensing

License model	Licensing per protected user
License scope	License without time limit including free upgrades and support for 1 year

NetOp® InHouse • Datasheet\_NNF\_DK\_250608 • All rights reserved



**Try now. Test the full version free for 30 days**  
[www.netop.com/freetrial](http://www.netop.com/freetrial)

