

Why is a Content-Filter needed?

It is important to control the content on the network and how your resources are being used. Often employees will tend to do private or illegal things in the work hours, due to boredom or other reasons. This will waste valuable work hours and can possibly put you at risk if your network is being abused for downloading copyrighted materials.

What does the Content-Filter consist off?

Included modules in the Content-Filter:

- Anti-Free Mail – This blocks access to official free email providers such as Hotmail, Yahoo Mail, Google mail etc. The use of free email providers can often indicate employees checking their private email in working hours
- Anti-Game – It is often a tempting to play network games such as Counter-Striker or other addictive games in work hours.
- Instant Message Recording – This provide monitoring of the usage of MSN Instant Messaging to see if your employees are communicating with your Business customers or with their friends.
- Anti-Instant Message – If your security policy is NO Instant Messaging this module blocks the use of programs such as MSN, Yahoo, Google Talk, Skype chat.
- Anti-VoIP – This allows blocking services like Skype, Yahoo Talk, Google Talk, VoIP usage and more. Employees can be talking privately in work hours or leak sensitive information without your knowledge
- Anti-P2P – If your security policy is block all P2P File Sharing services like BitTorrent, eDonkey2000, Emule, Kazaa and Napster enabling this module just do that for you. Those programs are often used to share copy righted materials such as music or movies. If this done in your corporate perimeter this will be your responsibility if a raid is being done. In some countries they will close down the Internet Connection in such a case so it can be a costly affair.
- File Filter – This option blocks downloading of specific file formats such as *.exe *.zip *.rar files conforming to the user's choice. This applies to emails, web browsing and other protocols.
- Protocol Filter – This allows blocking of specific protocols in your network. In some locations POP3 traffic is forbidden since this is often used by employees to check their private email in working hours. You can customize which protocols to block.
- Block Web Sites – This allows blocking of websites of your choice. Often employees will spend hours daily to read news sites, gossips, and websites of private interest in working hours.