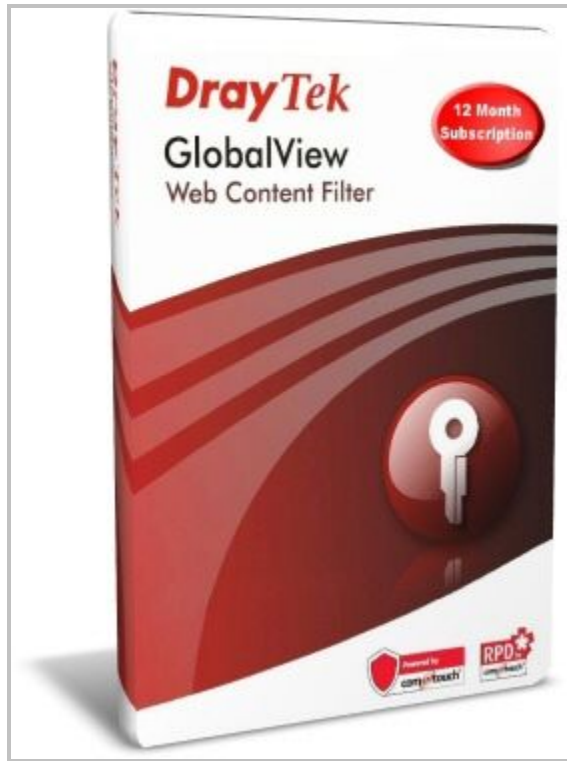


Web Content Filtering



DrayTek's Web Content Filtering (WCF) facilities enable you to protect your network and your users from web content according to your preferences. There are many reasons for doing this, for example:

Reason to Block	Example
Unsuitable	Adult material for children
Undesirable	Time wasting sites for employees
Dangerous	Malware or virus-ridden web sites
Fraudulent	Confidential data leaving your network

As DrayTek WCF is performed by your router - your point of entry to the Internet - it is far more difficult to circumvent than software solutions installed on each client/PC and applies to guest PCs too (laptops etc.). Blocking/filtering can be selective for certain computers, users or groups too, so that, for example, managers can have less filtering imposed than other users and time schedules can apply these content filtering for specific time periods only (the facilities and granularity of this depends on the specific model of router selected).

Internet Control for families and children

Whilst the Internet can be hugely beneficial to any family users, both for adults and children, there is also the opportunity for it to become distracting, over-consuming as well as risky. For children, a common use

of control control is to block inappropriate content, such as web sites with sexual, violent or other adult-oriented content in schools or anywhere else that children might use the Internet. That's the inappropriate content, but even age-appropriate content can be undesirable. Facebook might be great for your teens, and CBeebies for your younger children, but not if they are supposed to be doing something else. Many parents want to control access to the Internet, for example allowing access to acceptable web sites for specified times of day only. For your adult users in the home, you may want to block access to sites which have a high probability of being infected with malware. You may also wish to block your own computers from sending emails in case of trojan/zombie infection. There are infinite combinations of content filtering and firewalling you might want to impose in your home.

Staff Internet Abuse - A real cost to your business

The Internet provides your business with an effective, useful and often essential facility. Your staff can use it to find quick answers, liaise with customers, send and receive emails and many other productive tasks. Unfortunately, the Internet also provides the opportunity for mis-use. DrayTek products can help you restrict, control and monitor staff Internet usage.

Staff using your Internet facility for time-wasteful activities are costing you. Even more importantly these activities can put your businesses computers and network at risk. A recent survey of 10,000 employees indicated that 44% admitted to spending time on the Internet for personal use, for up to 2.1 hours per day.

Most staff are responsible and prudent with their Internet use and we always recommend a suitable AUP (Acceptable Use Policy) to be in place so that staff or any users of your systems know what they are and aren't permitted to use the computers for. This AUP can be re-inforced by DrayTek routers which can block specific content (either at certain times only or all times) and also block potentially harmful file/code types from being installed by rogue web sites. There are some staff who will make severe abuse of the Internet facilities - spending literally hours on personal matters or social networking sites.

Top 5 Personal Internet Uses for Employees

- Personal Email: Hotmail, Gmail, Yahoo etc.
- Instant Messaging: Skype, AOL, Yahoo etc.
- Social Networking: Facebook, MySpace, Twitter etc.
- Buying: Using Amazon, Ebay etc.
- Multimedia : YouTube, iPlayer etc.

It's easy to let a 'quick visit' become a prolonged stay without realising and losing track of time. All of the above activities can be immensely time consuming and addictive. What doesn't quite make the list but could be even more serious in its consequences is adult or illegal material being accessed in the workplace, as well as the higher likelihood that such sites are infected with malware which will then get onto your business network. There is also the potential to 'innocently' download software and install it on local PCs, unwittingly introducing spyware or trojans onto your network.

Introducing DrayTek Web Content Filtering

DrayTek Web Filtering allows you to block web content in four main ways:

1. By matching keyword / specific sites
2. By web site category (Subject to Subscription)
3. By digital content type
4. IP Filtering (Actually part of the firewall, along with many other security features.)

Features 1,3 and 4 above are included with the router. Feature 2 is included but requires an annual subscription to the external server which keeps a real-time constantly updated database of web sites. More details of that later. Features supported varies with router model; please check on specification for confirmation of Web Content Filter capabilities.

1. Keyword Matching URL Content Filter

In Keyword Matching you can specify a list of either banned (blacklist) or permitted sites (whitelist). The DrayTek method is 'object' oriented, which means that you create lists of keywords or sites, can then group them and then apply them into specific user groups or time periods

Using a *blacklist*, all sites would be accessible by your users except those that match the keywords you specify. This would be useful, for example where there are specific sites known to be causing disruption or timewasting in your organisation such as social networking or webmail. The example below would allow access to all sites except the ones listed:

Objects Setting >> Web URL Blacklist

Index	Name	
1.	WebMail Sites	hotmail gmail yahoo
2.	Social Networking	Facebook Twitter MySpace
3.		
4.		

A whitelist, on the other hand, is much more restrictive on what your users can access as it blocks all web sites by default and then only allows access to web sites which match your keywords. This is useful when you really want to lock down your Internet access to only allow very specific web site access. The example below would block access to all web sites except those listed:

Objects Setting >> Web URL Whitelist

Index	Name	
1.	News Sites	bbc reuters cnn
2.	Finance Sites	ft.com google.co.uk/finance finance.yahoo.com
3.	Markets	bloomberg.com moneyweek.com ftse.com
4.		

The URL blacklist and whitelist feature support varies with router model; Please check on specification for details of keyword matching support.

2. Web Site Category (DrayTek GlobalView, powered by Cyren)

DrayTek's GlobalView is built into most of our routers and allows you to select specific categories of web site which your router will allow access to. For example, an office may wish to block access to social networking or other company time-wasting sites or a home user might want to block adult sites from their children. In public Internet access facilities, you might want to block various unsuitable categories. GlobalView covers 64 separate categories which you can select as blocked or permitted. Every time one of your users attempts to access a site, the router's automatically queries the central GlobalView server to ascertain its classification. This takes only milliseconds. If a site is blocked by GlobalView, according to the categories you have selected, instead of the requested web page, a warning message is displayed to the user (you can customise the message).

The GlobalView central database is continuously updated with new sites and changes to sites but also records normally legitimate sites which have become compromised or contain malware (a unique feature to GlobalView). Access to the GlobalView server requires an annual subscription. A free 30-day trial is included with all new routers so that you can try the feature out before subscribing. Scroll down the box below to see the 64 different categories which can be blocked by GlobalView, either permanently or at certain times of day/week according to your chosen schedule and for the PCs you choose.

GlobalView Categories :

Globalview requires a subscription to the Globalview server. This is a 12-month subscription available from your dealer. There is no additional licensing for the number of users you have; it is a flat fee based on your router model:

Subscription Type	Supported Series	EAN
Group A / WCFA	Vigor 2820, 2830, 2832, 2850, 2860, 2920, 2925, 3200, PBX2820, BX-2000	47198535537 67
Group B / WCFB	Vigor 2110, 2130, 2710, 2750, 2760	47198535538 28
Group S / WCFS	Vigor 3300V+, 300B, 2930, 2960, 2950, 2955, 2952, 3220, 3510, 3900, 5510	47198535543 06

<input type="checkbox"/> Alcohol & Tobacco	<input checked="" type="checkbox"/> Criminal Activity	<input checked="" type="checkbox"/> Gambling
<input type="checkbox"/> Hate & Intolerance	<input checked="" type="checkbox"/> Illegal Drug	<input checked="" type="checkbox"/> Nudity
<input type="checkbox"/> Porn & Sexually	<input checked="" type="checkbox"/> Violence	<input checked="" type="checkbox"/> Weapons
<input type="checkbox"/> School Cheating	<input checked="" type="checkbox"/> Sex Education	<input checked="" type="checkbox"/> Tasteless
<input type="checkbox"/> Entertainment	<input type="checkbox"/> Games	<input type="checkbox"/> Sports
<input type="checkbox"/> Travel	<input type="checkbox"/> Leisure & Recreation	<input type="checkbox"/> Fashion & Beauty
<input type="checkbox"/> Business	<input type="checkbox"/> Job Search	<input type="checkbox"/> Web-based
<input checked="" type="checkbox"/> Chat	<input checked="" type="checkbox"/> Instant Messaging	
<input type="checkbox"/> Anonymizers	<input checked="" type="checkbox"/> Forums & Newsgroups	<input checked="" type="checkbox"/> Computer
<input type="checkbox"/> Download Sites	<input checked="" type="checkbox"/> Streaming, Downloads	<input checked="" type="checkbox"/> Phishing & Scams
<input type="checkbox"/> Search Engine, Portals	<input checked="" type="checkbox"/> Social Networking	<input checked="" type="checkbox"/> Spam Sites
<input type="checkbox"/> Malware	<input checked="" type="checkbox"/> Botnets	<input checked="" type="checkbox"/> Hacking
<input type="checkbox"/> Illegal Software	<input checked="" type="checkbox"/> Information Security	<input checked="" type="checkbox"/> Peer-to-Peer

Why Globalview?

Globalview, powered by Cyren, uses a unique method of categorisation to ensure the most accurate, relevant and up to date database of web sites. In particular compared to other services, these are some important advantages of Globalview:

1. Globalview is built into the hardware. There are software solutions for category blocking or parental control but they have to be installed on each PC, maintained on each PC and someone with the right skills (a skilled employee or smart child!) can often find a way to bypass or disable the software. DrayTek's Globalview operates at your Internet point of entry so examines all web site URLs requested and cannot be turned off without administrative rights to the router.
2. GlobalView is a commercial/professional Service
3. . Unlike some other services, GlobalView does not rely on volunteers to submit suggestions for sites to include or rely on volunteers to categorise each site submitted (and multiple users to then concur which the category proposal). Relying on community-driven categorisation can lead to inaccuracies, delays, mischief and an incomplete database which omits many sites, particularly those which are more obscure or unknown (which are also more likely to be undesirable). The Globalview WCF service has been available for many years, and continuously evolves to improve performance and accuracy.
4. GlobalView is not a Domain Resolution Service, therefore it is not possible to bypass it merely by changing the DNS settings on your PC, or by browsing by IP address instead of URL. Globalview intercepts and examines all web requests for their specific destination rather than just intercepting DNS requests and rejecting those which it believes should be blocked.
5. Categorisation uses an automated mechanism.
6. GlobalView URL filtering is based on a hugely scalable cloud-based architecture that uses the extensive cloud computing resources available for categorization. GlobalView URLF

uses a dynamically built, relevant local database with real-time connectivity to a hugely scalable cloud-based repository. GlobalView URLF therefore provides more complete, relevant categorization of the Internet. GlobalView's main benefit is the highly intelligent and accurate categorisation algorithms which are used to build its database.

7. Zero-Hour Protection
8. The Internet is a living, continuously growing and evolving system. As GlobalView operates in real-time, it can categorise a site from the moment it becomes available from the first time it is requested, and re-categorise it if it changes at a later date without community-driver or user intervention. Users do not have to manually submit sites for categorisation.
9. Categorise IP Addresses
10. Some other content filtering services can be bypassed simply by the user browsing to an IP address so that the URL is never considered/checked. Globalview will categorise sites based on their IP address if a user tries to access via that method. i.e. Both www.facebook.com and 69.63.190.18 would be blocked by GlobalView if you have prohibited social networking. This is also particularly useful in combating phishing emails which commonly use IP addresses instead of URLs. The DrayTek router can, in addition, block browsing by IP address altogether.
11. Multiple Categories Per Site
12. Globalview can identify a single web site or page as falling into several categories, for example a site might provide both 'dating' and 'adult' content so if you choose to block either of those, Globalview will correctly identify it as both.
13. Site granularity
14. Whereas other services considers only the top level domain (TLD) i.e. the URL up until the first "/", Globalview will parse/consider the whole URL. This is particularly a problem for Web 2.0 sites such as blog sites (members.tripod.com/sitename) where one user's blog might be for kids and other user's contain adult-suited material. Another example is commercial sites which contain different materials types. For example, Globalview will distinguish between "sportsillustrated.cnn.com" (Sports pages) and "sportsillustrated.cnn.com/swimsuit/" (Swimwear models/nudity).
15. Embedded Links are examined.
16. Another common methods that users might use to bypass web controls is using parsing or translation web sites. For example, if you try to visit "<http://translate.google.com/translate?tl=it&u=http%3A%2F%2Fwww.swimwearplace.com%2F>" then GlobalView will correctly identify that you have asked Google to display 'www.swimwear.com' and block it if that is a category you have prohibited, whereas other services will just see 'Google' and permit access based on the categorisation of Google (search engine).

3. Digital Content Type

DrayTek's Content filtering allows you to specify particular data types or web content to be blocked by the router. The vigor is pre-set with many different content types or protocols. You can select any or all

of them for blocking. There are infinite combinations but some examples of commonly blocked content are:

- Block download of executable (EXE) or compressed (ZIP) files to reduce the chance of virus infection or installation of untested software.
- Block Peer-to-Peer (P2P) software such as BitTorrent, to avoid users using vast amounts of your bandwidth or engaging in media piracy.
- Block HTTP/FTP upload or webmail to prevent theft/espionage of your company data
- At Home, block Instant Messaging protocols to prevent your children from unsupervised chat with strangers.
- Block SMTP from all devices other than your mail server to stop Trojan Zombies

For detailed list on the protocols and content type which can be blocked, [Click Here](#).

4. IP Filtering

This is a more technically complex method. All data sent across the Internet is sent as a 'data packet' between devices (for example between your PC and a web site) Each device has its own IP address (such as '194.194.123.18'). In addition, each data packet can be one of several data types (TCP, UDP, ICMP etc.) and may also have additional information such as TCP port numbers. Don't worry if this all sounds a bit complicated; the useful factor here is that these packets can be distinguished and therefore rules can be set up on the router to block or pass packets which match parameters you choose.

Examples of useful IP filters might be to block incoming mail from all but known mail servers, or to allow access to your internal web server from all addresses except known remote locations. IP Filters can be nested so that a chain of filters can all be tied together and data passed only if one of, or all of the rule criteria are met. As we said, it's a technically complex feature but immensely powerful.

Note : Although we include IP filtering here, most users actually consider that to be part of the main firewall features as it's not filtering 'by content' as such.

SSL/TLS ("HTTPS") Sites & DrayTek DNS Filter

Concerns regarding privacy and security have increasingly lead to web sites moving their services to web servers that offer SSL/TLS connections as standard. SSL/TLS connections are those prefixed with https:// or commonly shown with a 'padlock' symbol in your browser.

SSL/TLS is a protocol that allows communication to be secured encryption so that it can't be read by a third party - anyone in between you and the server. This security also extends to the actual URL (web address) that the user enters, which has an impact on web content filtering methods that categorise websites based on the URL that is being accessed.

The Keyword matching URL Content Filter is unable to make web content filtering decisions for HTTPS requests because the web address is encrypted. DrayTek's Globalview is also affected but the Globalview servers have other methods which can assist with categorisation decisions even when the URL is encrypted.

However a new feature is now available on various DrayTek products called DNS Filter.

When a PC tries to access a web site, it has to always convert that web address into an IP address (e.g. 194.213.12.44). That IP address itself cannot be encrypted by SSL/TLS because your router has to know where to send the data to!

DrayTek's new DNS Filter examines all DNS lookups that your PCs make and then make categorisation or content filtering decisions. DNS Filter can be used with both the Keyword matching URL filter (whitelists/blacklists) and the Globalview Web Content filter.