English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

Access Restrictions allows you to create a set of rules that govern internet access to machines on your network. You can create rules that govern access by individual IP or MAC address, IP address range, time-of-day, traffic type, URL and keywords, etc.

You can create up to 10 sets of rules, with each set of rules being referred to as a **policy**. A policy can contain multiple individual rules, such as filtering a specific machine access to a particular web site, and/or filtering access to certain unwanted P2P protocols.

Remember that all policies will be used (this is different than in factory Linksys firmware where only the first matched is used)! For example, if policy #1 is a **Deny** policy that restricts all internet access to a machine on your LAN, that machine will no longer be able to access the Internet, regardless of any Filter policies you might have. *Note: The term "Filter" is erroneously labeled as "Allow" in earlier versions of DD-WRT firmware. This is the main source of confusion when dealing with access restrictions in DD-WRT. See Eko's forum post for more information.*

The **Filter** option is used to block access to web sites, services, or keywords. However, it does not block internet altogether like the "Deny" option does. Nor does it allow internet access during times that a Deny policy denies it.

If you will notice, when you click the "Deny" button (instead of the Filter button), those extra options at the bottom of the page get greyed out (at least in newer dd-wrt versions). This is because filtering a web site, service, etc. in a Deny policy is pointless since the machines in the policy would be denied internet access anyway!

Contents

Denying Internet Access

1. Select an unused policy number (1-10) in the drop-down menu.
2. Enable your policy by setting *Status* to *Enable*.
3. Enter a name for your policy in the *Policy Name* field. Ex. "Deny Internet"
4. Click the *Edit List of clients* button.
5. On the *List of clients* screen, specify clients by IP address or MAC address. Enter the appropriate IP addresses into the *IP* fields. If you have a range of IP addresses to filter, complete the appropriate *IP Range* fields. Enter the appropriate MAC addresses into the *MAC* fields.
6. Click the *Save* and *Apply* buttons to save your changes. Click the *Close* button to return to the *Access Restrictions* screen.

7. Click the radio button next to *Deny* Internet access for listed clients during selected days and hours.
8. Set the days when internet access will be denied. Select *Everyday* or the appropriate days of the week.
9. Set the time when internet access will be denied. Select *24 Hours*, or check the box next to *From* and use the drop-down boxes to designate a specific time period.
10. Click *Save* and *Apply*.
11. To create or edit additional policies, repeat the necessary steps above.

NOTE If defining a policy that extends into the next day, you must specify two separate policies

Filtering Services/URLs/Keywords

For more advanced content filtering try OpenDNS

1. Select an unused policy number (1-10) in the drop-down menu.
2. Enable your policy by setting *Status* to *Enable*.
3. Enter a name for your policy in the *Policy Name* field. Ex. "Filter Bittorrent"
4. Click the *Edit List of clients* button.
5. On the *List of clients* screen, specify clients by IP address or MAC address. Enter the appropriate IP addresses into the *IP* fields. If you have a range of IP addresses to filter, complete the appropriate *IP Range* fields. Enter the appropriate MAC addresses into the *MAC* fields.
6. Click the *Save* and *Apply* buttons to save your changes. Click the *Close* button to return to the *Access Restrictions* screen.
7. Click the radio button next to *Filter* Internet access for listed clients during selected days and hours. (Remember, many DD-WRT versions will have an "Allow" option, but it really means "Filter")
8. Set the days when access will be filtered. Select *Everyday* or the appropriate days of the week.
9. Set the time when access will be filtered. Select *24 Hours*, or check the box next to *From* and use the drop-down boxes to designate a specific time period.
10. Under *Blocked Services*, enter the services you wish to block (if any).
11. Under *Website Blocking by URL Address*, enter in the domain name(s) you wish to block (if any).
12. Under *Website Blocking by Keyword*, enter the keywords you wish to block (if any).
13. Click *Save* and *Apply*.
14. To create or edit additional policies, repeat the necessary steps above.

Note: Filtering does not work if you don't enter a list of clients for that policy.

Delete

To delete an Internet Access Policy, select the policy number and click the Delete button

Summary

To see a summary of all the policies, click the Summary button. The Internet Policy Summary screen will show each policy's number, Policy Name, Days, and Time of Day. To delete a policy, click its box, and then

click the Delete button. Click the Close button to return to the Filters screen.

Filtered Internet Port Range

To filter PCs by network port number, select Both, TCP, or UDP, depending on which protocols you want to filter. Then enter the port numbers you want to filter into the port number fields. PCs connected to the Router will no longer be able to access any port number listed here. To disable a filter, select Disable.

Filtering Inbound Traffic

See Iptables command.

Problems/Issues?

Still having problems with Access Restrictions? You may be using an older and no longer maintained version of DD-WRT firmware. In that case, it may help to review the steps in an older revision of this article, before it was modified for use with DD-WRT v24+