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

OpenDNS ??????DNS????????????????????????????? By simply using their DNS servers instead of your ISP's you are automatically protected from their list of Phishing websites. However, in order to restrict a variety of adult website content you will need to create a free account with them, register your IP address and select the categories you want restricted (i.e. sexuality, nude, pornography, lingerie, grotesque, etc...). Since most of us have DHCP assigned WAN IP addresses that change periodically we need to instruct our router to tell OpenDNS what our new IP address is when it changes. We will go over that below.

Contents

- 1 ????
- 2 OpenDns with DNS-O-Matic for users with a Dynamic IP
- 3 DNS????
- 4 ?????IP?IP???DNS??
- 5 ?????

????

1. On the **Setup** tab under **Network Address Server Settings (DHCP)** look for **Static DNS 1** and **Static DNS 2**
2. Set **Static DNS 1** to **208.67.222.222**
3. Set **Static DNS 2** to **208.67.220.220**
4. Depending on the behavior you want: either leave **Static DNS 3** set to **0.0.0.0** to still fall back to your ISP DNS if OpenDNS is unresponsive, set it to **10.0.0.0** (a non-usable IP) if you don't want to use any other servers, or set it to another DNS server of your choice. Do not duplicate one of the other DNS IP's or else it will act the same as if you left it set to 0.0.0.0.
5. Apply Settings and go to the **Services** tab
6. Under **DNSMasq** put **strict-order** in the **Additional DNSMasq Options** text box if you want the DNS servers to be queried in the order they're listed rather than randomly.
7. Apply Settings again

OpenDns with DNS-O-Matic for users with a Dynamic IP

OpenDNS provides an additional service for users with Dynamic DNSs. Their DNS-O-Matic will relay the request to OpenDNS and also optionally forward this to any number of additional Dynamic DNS providers.

1. Follow instructions for basic setup above.

DNS-O-Matic with dd-wrt

2. Setup an account with OpenDns and **Enable dynamic IP update** under the settings tab on the OpenDNS website. Also enable any filtering options you want.
3. Log into DNS-O-Matic. It shares the same username and password for OpenDNS.
4. Add OpenDNS as a service on DNS-O-Matic
5. Also add account information for any other Dynamic DNS providers you have.
6. Now click the "Update Info" radio buttion
7. On the **DDNS** tab under **Setup** in dd-wrt set **DDNS Service** to Custom.
8. Set **DYNDNS Server** to updates.dnsomatic.com
9. Fill in your Username and Password for OpenDNS/DNS-O-Matic
10. Set **Host Name** to all.dnsomatic.com
    - To update multiple hosts, use ***hostname1*** **-a** ***hostname2*** **-a** ***hostname3*** **-a** ***hostnameN*** Source: this tip.
11. Put /nic/update?hostname= in the **URL** text box.
    - If that doesn't work, use:

      ```
      http://updates.dnsomatic.com/nic/update?hostname=
      ```
    - If you get a badauth error from dnsomatic, it could be that you need to use https instead of http, so try:

      ```
      https://updates.dnsomatic.com/nic/update?hostname=
      ```
12. Apply

DNS????

You can prevent users from using their own DNS servers (and hence get around content filtering) by intercepting DNS queries and forcing them to use the DNS servers you specify.

1. Go to the **Commands** tab under **Administration**.
2. In the **Commands** box paste the following:

```
iptables -t nat -A PREROUTING -i br0 -p udp --dport 53 -j DNAT --to `nvram get lan_ipaddr`
iptables -t nat -A PREROUTING -i br0 -p tcp --dport 53 -j DNAT --to `nvram get lan_ipaddr`
```

1. Click **Save Firewall** (note: your WAN interface will be restarted)

?????IP?IP???DNS??

Same as above but for a specific IP address/Range

1. Go to the **Commands** tab under **Administration**.
2. In the **Commands** box paste the following:

```
iptables -t nat -A PREROUTING -i br0 -s 192.168.1.128/25 -p udp --dport 53 -j DNAT --to $(nvram g
iptables -t nat -A PREROUTING -i br0 -s 192.168.1.128/25 -p tcp --dport 53 -j DNAT --to $(nvram g
```

?

```
iptables -t nat -I PREROUTING -i br0 -s 192.168.1.128/25 -p udp --dport 53 -j DNAT --to 208.67.22
iptables -t nat -I PREROUTING -i br0 -s 192.168.1.128/25 -p tcp --dport 53 -j DNAT --to 208.67.22
```

1. Click **Save Firewall** (note: your WAN interface will be restarted)

?????

Do note that many major websites, download hosts and media sites are now using content delivery network. These network will resolve an IP that is closest to you for performance. Typically, when you use your ISP's DNS server, you will get an IP address within or close to your ISP's network.

???????OpenDNS???????????OpenDNS?'????????????IP????????????????????????