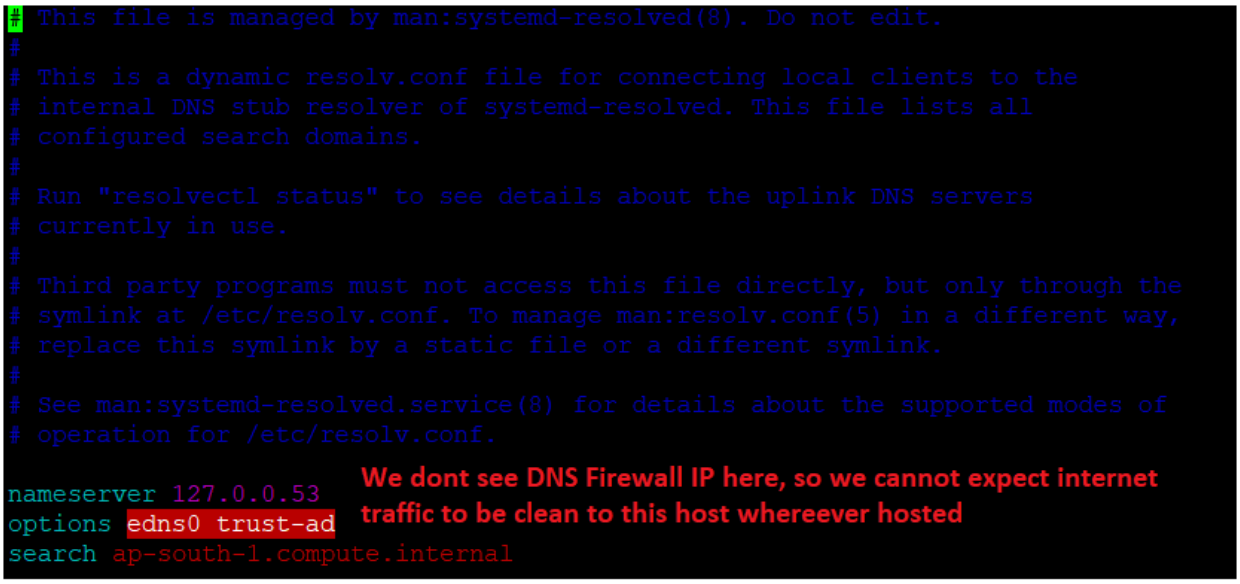
Hardcode DNS Firewall or Sinkhole IP in Ubuntu Host

Important file /etc/resolv.conf




```
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search ap-south-1.compute.internal
```

Say we need to edit this file to point to OpenDNS Family Shield DNS Firewall IP address 208.67.222.123 and 208.67.220.123 (or any DNS Firewall IPs you wish),

nameserver 208.67.222.123
nameserver 208.67.220.123

If we just manually apply it above line nameserver 127.0.0.1 , whenever the host reboots or network services or the adapter restarts, whatever manually applied to /etc/resolv.conf will roll back automatically , meaning our changes will not take effect.

To perform Hardcode DNS Firewall or Sinkhole IP in Ubuntu Host, please follow the below steps,

Check the below command in the terminal,

sudo systemctl status resolvconf.service

```
root@ip-172-31-35-90:~# sudo systemctl status resolvconf.service
Unit resolvconf.service could not be found.
root@ip-172-31-35-90:~#
```

Since the resolvconf.service is not available, lets install the service,

sudo apt install resolvconf -y

If we check the resolvconf.service now, it should work.

```
root@ip-172-31-35-90:~# sudo systemctl status resolvconf.service
● resolvconf.service - Nameserver information manager
     Loaded: loaded (/lib/systemd/system/resolvconf.service; enabled; venc
     Active: active (exited) since Thu 2023-02-02 09:41:54 UTC; 1min 39s a
       Docs: man:resolvconf(8)
   Main PID: 4599 (code=exited, status=0/SUCCESS)
      Tasks: 0 (limit: 4689)
     Memory: 0B
     CGroup: /system.slice/resolvconf.service

Feb 02 09:41:54 ip-172-31-35-90 systemd[1]: Started Nameserver informatior
Feb 02 09:41:54 ip-172-31-35-90 resolvconf[4604]: /etc/resolvconf/update.c
```

Run these below commands once,

sudo systemctl start resolvconf.service

sudo systemctl enable resolvconf.service

sudo systemctl status resolvconf.service

Edit the file /etc/resolvconf/resolv.conf.d/head to add the OpenDNS Family Shield DNS Firewall IPs

sudo vi /etc/resolvconf/resolv.conf.d/head

nameserver 208.67.222.123
nameserver 208.67.220.123

We need to update resolv.conf to use the new DNS Firewall IPs,

sudo resolvconf --enable-updates
sudo resolvconf -u

Now open /etc/resolv.conf to confirm our DNS Firewall IPs have been written,

sudo vi /etc/resolv.conf

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 208.67.222.123
nameserver 208.67.220.123

nameserver 127.0.0.53
search ap-south-1.compute.internal
options edns0 trust-ad
```

New DNS Firewall IPs are updated

Soon after checking /etc/resolv.conf file , when you come out of the file (quit) , you may get the below error,

```
root@ip-172-31-35-90:~# sudo vi /etc/resolv.conf
sudo: unable to resolve host ip-172-31-35-90: Name or service not known
root@ip-172-31-35-90:~#
```

Note the hostname from the error,

```
root@ip-172-31-35-90:~# hostname
ip-172-31-35-90
root@ip-172-31-35-90:~#
```

Now goto /etc/hosts and do the changes like the below,

```
127.0.0.1 localhost
```
Change 'localhost' to ip-172-31-35-90

```
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Now again goto file /etc/resolv.conf and test , you will not get the error sudo: unable to resolve host ip-172-31-35-90: Name or service not known anymore.

```
root@ip-172-31-35-90:~# vi /etc/resolv.conf
root@ip-172-31-35-90:~#
root@ip-172-31-35-90:~#
```

Finally lets do a host reboot test shutdown -r now, so that /etc/resolv.conf shows only DNS Firewall IPs.

Once the reboot is complete, when we check the file /etc/resolv.conf ,

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 208.67.222.123
nameserver 208.67.220.123

nameserver 127.0.0.53
search ap-south-1.compute.internal
```

```
root@ip-172-31-35-90:~# nslookup google.com
Server:         208.67.222.123
Address:        208.67.222.123#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.183.14
Name:   google.com
Address: 2404:6800:4009:820::200e

root@ip-172-31-35-90:~#
```

DNS Firewall IP is the resolver of this host.

The output is as expected. Once we quit the file , the error also did not appear.

```
root@ip-172-31-35-90:~# vi /etc/resolv.conf
root@ip-172-31-35-90:~#
```

Done!!!