

# Mullvad VPN App 4.2 setup guide

---

[solene](#) 1 March 15, 2024, 3:03pm

## Intro

This guide explains how to setup a VPN with Mullvad app on Qubes OS 4.2 using a Fedora template.

Mullvad app is open source and they provide repositories for fedora / debian, there are no documentation to deploy the App, only an official page explaining [how to setup WireGuard](#), or a community guide for [Mullvad WireGuard without the App](#)

The App supports OpenVPN and WireGuard tunnels. Bridge support is available for OpenVPN and WireGuard has obfuscation available, these features are useful if you are unable to connect due to censorship.

They seem also a legit service to use as per the trustable source [Private VPN Service Recommendations and Comparison, No Sponsors or Ads - Privacy Guides](#)

## Setup

### Qube creation

- Create a dedicated qube for the vpn
  - Name it as you want (I will name it sys-vpn-mullvad-app)
  - Choose type “Standalone” with the template fedora-39 (or xfce flavor, minimal flavor should work too)
  - Check “provide network access to other qubes” in the Advanced settings tab
- In the qube settings
  - Give it 800 MB of memory minimum
  - Add the service qubes-firewall

### Qube configuration

- Start the qube
- In the qube terminal, run:

```
sudo dnf config-manager --add-repo https://repository.mullvad.net/rpm/stable/mullvad.repo
sudo dnf install mullvad-vpn
```

- Reboot the qube

### Mullvad App

Start the App with `/opt/Mullvad\ VPN/mullvad-gui` or add “Mullvad VPN” application in the qube menu entry that should be available after the installation process.

The Mullvad VPN app should start without issue:

- Enter your credentials
- Configure the App as you want

Auto start at boot can be enabled in the settings.

## Fix DNS

**i** The App uses several custom DNS that change based on the options selected by the user, but this doesn't propagate to the qubes behind it, resulting in long latency times for resolving hostnames. The following script forces all DNS requests to automatically go through the selected custom DNS server.

**!** The script depends on `inotify`, which can be installed with the `inotify-tools` package.

Edit the file `/usr/local/bin/mullvad-dns.sh` to put the following content:

```
#!/usr/bin/env bash

update_dns() {
    # mullvad_on: 0 -> off, 1 -> on
    mullvad_on=$(( [ $(grep -v -c "nameserver \+10.139" /etc/resolv.conf) -gt 0 ] ] && echo 1

    if [ [ $mullvad_on -eq 1 ] ]; then

        echo "Mullvad is on"

        # get the mullvad dns ip address. First one is used if there is more than one.
        mullvad_dns_ip=$(grep "nameserver" < /etc/resolv.conf | awk '{print $2}' | head -n 1)

        # delete all the lines defined in dnad-dns
        sudo nft flush chain ip qubes dnad-dns

        # forward all dns requests to mullvad dns servers
        sudo nft add rule ip qubes dnad-dns meta l4proto { tcp, udp } ip daddr { 10.139.1.1,

    else

        echo "Mullvad is off"

        # get qubes nameserver ip addresses
        nameserver_ips=$(grep "nameserver" < /etc/resolv.conf | awk '{print $2}')
```

Make the script executable

```
sudo chmod +x /usr/local/bin/mullvad-dns.sh
```

And add this to run the script at boot time to `/rw/config/rc.local`

```
/usr/local/bin/mullvad-dns.sh &
```

## Avoid issues with WireGuard

**i** WireGuard tunnels can trigger a MTU issue in the network, in short it could make some websites not working (like duckduckgo) because of too big packet sizes. This is a common issue with WireGuard VPNs.

Add this to `/rw/config/qubes-firewall-user-script`

```
nft add rule ip qubes custom-forward tcp flags syn / syn,rst tcp option maxseg size set rt m
```

This will automatically ensure that the qubes network packets will fit in a WireGuard network packet and will make things work.

## Killswitch configuration (easy method)

**i** You may want to force all qubes traffic to go through the VPN and block non-VPN traffic. Mullvad app offers a killswitch but the app could still crash and the killswitch wouldn't be guaranteed to work.

**i** This easy method plays well with the App as you don't need to configure a firewall rule for each server/port. However, if the qube gets compromised it's possible to disable the rule, if you want more security against this

threat you should use `qvm-firewall`.

Add the rules below in `/rw/config/qubes-firewall-user-script` in the qube:

```
# Prevent the qube to forward traffic outside of the VPN
nft add rule qubes custom-forward oifname eth0 counter drop
nft add rule ip6 qubes custom-forward oifname eth0 counter drop
```

6 Likes

---

[Qubes 4.2 and mullvad/wireguard problem](#)

---

[Does it make sense to set up system wide Mullvad?](#)

---

[Anyone got an AppVM or Debian standalone solution for Mullvad VPN?](#)

---

[Need a current working Mullvad VPN guide for Qubes 4.2.1](#)

---

[Is there value in a disposable VPN qube?](#)

---

[Static MAC address but only a connection in sys-net](#)

---

[Mullvad VPN setup guide](#)

---

[Understanding VPN ProxyVM](#)

---

[Brave and Vivaldi don't connect to internet with mullvad vpn](#)

---

[How can I open an Application via dom0 keyboard shortcut?](#)

---

[Mullvad VPN qube using qubes-task DNS problem](#)

---

[Mullvad VPN for all traffic](#)

---

[Chain vpn -> tor safety](#)

---

[Qubes VPN](#)

---

[Anyone got an AppVM or Debian standalone solution for Mullvad VPN?](#)

---

[Understanding VPN ProxyVM](#)

---

[Understanding VPN ProxyVM](#)

---

[curbs94](#) 2 March 15, 2024, 11:12pm

Have you looked at [this guide](#) which uses an AppVM instead of standalone?

1 Like

---

[solene](#) 3 March 16, 2024, 6:58am

Nope, thanks for sharing.

If someone only uses a single instance of Mullvad app, the template increases the setup complexity, but it's useful when you need multiple instances.

I'm curious to see the DNS tricks works, I've had no success with `/usr/lib/qubes/qubes-setup-dnat-to-ns`

---

[DVM 4](#) March 16, 2024, 1:53pm

Mullvad uses many different DNS addresses depending on what the user selects in the app. The default Wireguard DNS address is `10.64.0.1`, but it can also be in the `100.64.0.x` range if the user chooses to use the [DNS filtering rules](#).

For OpenVPN, it's different too. Each port gives a different subnet and the DNS is always `10.x.0.1`. DNS filtering (`100.64.0.x`) also works with OpenVPN.

Since it's hard to know what protocol the user will be using and if they will be using any DNS filtering rules, I would recommend adding the following script to update the DNS accordingly:

```
#!/usr/bin/env bash

update_dns() {
    # mullvad_on: 0 -> off, 1 -> on
    mullvad_on=$(( [[ $(grep -v -c "nameserver \+10.139" /etc/resolv.conf) -gt 0 ] ] && echo 1

    if [[ $mullvad_on -eq 1 ]]; then

        echo "Mullvad is on"

        # get the mullvad dns ip address. First one is used if there is more than one.
        mullvad_dns_ip=$(grep "nameserver" < /etc/resolv.conf | awk '{print $2}' | head -n 1)

        # delete all the lines defined in dnad-dns
        sudo nft flush chain ip qubes dnad-dns

        # forward all dns requests to mullvad dns servers
        sudo nft add rule ip qubes dnad-dns meta l4proto { tcp, udp } ip daddr { 10.139.1.1,

    else

        echo "Mullvad is off"

        # get qubes nameserver ip addresses
        nameserver_ips=$(grep "nameserver" < /etc/resolv.conf | awk '{print $2}')
```

1 Like

---

[jagnopurka](#) 5 March 16, 2024, 3:05pm

Mullvad has their own guide specifically for Qubes: [Mullvad on Qubes OS 4](#)

However it doesn't allow to easily change VPN server on the fly

solene:

```
# Prevent the qube to forward traffic outside of the VPN
nft add rule qubes custom-forward oifname eth0 counter drop
nft add rule ip6 qubes custom-forward oifname eth0 counter drop
```

I would feel better if a killswitch was whitelist-based instead of blacklist-based like here. Maybe it would be better to drop everything by default and only allow packets on Mullvad's interface?

---

[solene](#) 6 March 16, 2024, 3:23pm

jagnopurka:

Mullvad has their own guide specifically for Qubes: [Mullvad on Qubes OS 4](#)

It was already linked in the guide, but they don't cover the App setup.

jagnopurka:

I would feel better if a killswitch was whitelist-based instead of blacklist-based like here. Maybe it would be better to drop everything by default and only allow packets on Mullvad's interface?

if you need a strong killswitch, do it with `qvm-firewall` that will apply the rules in the qube'Netvm, it's way more reliable.

1 Like

---

[Arka](#) 7 March 16, 2024, 4:15pm

Thank you for this tutorial,

you forgot quotation marks in the dns fix part

---

[frustrated\\_user](#) 8 March 28, 2024, 6:45pm

New Qubes user here. I struggled for a bit and want to clarify what I had trouble with for any other less experienced users.

I was thinking the DNS script wasn't working because Mullvad's leak checker kept telling me I was leaking. This was not because of the script DVM wrote, which works, but was actually from a Firefox browser setting.

When you do the leak check on mullvad's site and read the DNS leak guide, it has the answer. You have to disable "DNS over HTTPS" setting in Firefox ESR. By default it is enabled and made it so I was using a Cloudflare DNS server nearby the VPN server.

Also it wasn't clear to me by reading this thread, but the script DVM wrote needs to be run in the `sys-mullvad-vpn-app` qube terminal, not the `Dom0` terminal. The script needs to be run again if you change the settings in the DNS blocking inside the Mullvad app, however it seems like you don't need to run the script again just to change the VPN server if it has the same DNS blocking settings. The script also needs to be run again after reboot.

Could someone give specific instructions on how to set up the killswitch in the `qvm-firewall`? I barely know what I'm doing and don't want to break anything since I have the VPN working now.

Thank you all.

---

[\[Tutorial 4.2&4.1\] Mullvad Wireguard with Qubes](#)

---

[gubehead38](#) 9 April 5, 2024, 2:57pm

Big thanks for this guide. This is easy and fast and the gui helps a lot (edit. internet not working on browsers, but telegram app works?)

---

[qubehead38](#) 10 April 5, 2024, 5:11pm

solene:

```
/rw/config/qubes-firewall-user-script
```

nothing happens when i put this command in console.

---

[solene](#) 11 April 5, 2024, 5:27pm

qubehead38:

nothing happens when i put this command in console.

what did you add to that file? what do you expect when you run it?

---

[qubehead38](#) 12 April 6, 2024, 11:41am

I did this guide exactly same, same fedora version everyting.

Now the proxy vm which has mullvad gui app seems to somehow provide internet to app vm, because telegram app is working via mullvad vpn, and firefox mullvad extensions shows “connected to mullvad” status, and says the proxy is working... but the firefox can’t connect to any websites. Same with chrome and other app vms.

Wonder what is causing this?

---

[solene](#) 13 April 6, 2024, 12:29pm

can you try ping 9.9.9.9 and ping quad9.net in a terminal and say if both works?

If [quad9.net](#) doesn’t work, it’s likely there is a DNS issue. There is a DNS fix required in the guide.

---

[darkgh05t](#) 14 April 7, 2024, 4:16am

I have the exact same problem too.

ping 9.9.9.9 in the appvm works fine but ping [quad9.net](#) does not work ?

---

[solene](#) 15 April 7, 2024, 7:48am

did you do the DNS fix step?

### [Mullvad VPN App 4.2 setup guide](#)

Intro This guide explains how to setup a a VPN with Mullvad app on Qubes OS 4.2 using a Fedora template. Mullvad app is open source and they provide repositories for fedora / debian, there are no documentation to deploy the App, only an official page explaining [how to setup WireGuard](#), or a community guide for [Mullvad WireGuard without the App](#) The App supports OpenVPN and WireGuard tunnels. Bridge support is available

for OpenVPN and WireGuard has obfuscation available, these features are usefu...

---

[darkgh05t](#) 16 April 7, 2024, 8:15am

yes i added the script with the DNS fix but still not working on the browsers in appvm

---

[solene](#) 17 April 7, 2024, 8:39am

what is the content of `/etc/resolv.conf` in the Mullvad qube?

---

[darkgh05t](#) 18 April 7, 2024, 8:49am

`nameserver 100.64.0.23`

---

[solene](#) 19 April 7, 2024, 8:50am

I just found a typo in my guide,

I wrote

```
DNS=10.64.01
```

instead of

```
DNS=10.64.0.1
```

Can you try to change this and reboot the mullvad qube? If it still doesn't work, try 100.64.0.23 instead of 10.64.0.1

1 Like

---

[darkgh05t](#) 20 April 7, 2024, 8:56am

yeah i noticed the typo earlier, i fixed that but still no go, I also changed the Ip to 100.64.0.23, but still not working ?

---

[solene](#) 21 April 7, 2024, 9:10am

did you reboot the qube after the change?

---

[darkgh05t](#) 22 April 7, 2024, 9:42am

yes,

could it be something with the MTU issues ?

---

[solene](#) 23 April 7, 2024, 10:13am

No, you clearly face a DNS issue here, the MTU isn't related.

I'm not sure what to do next to help you debug this... If you know how to use tcpdump/wireshark, it could be interesting to see what happens in the mullvad vpn when an AppVM make a DNS request.

---

[apparatus](#) 24 April 7, 2024, 10:20am

What's the output of this command in your VPN qube?

```
sudo nft list table ip qubes
```

1 Like

---

[IVPN App 4.2 setup guide](#)

---

[darkgh05t](#) 25 April 7, 2024, 11:05am

```
table ip qubes {
  set downstream {
    type ipv4_addr
    elements = { 10.137.0.10 }
  }

  set allowed {
    type ifname . ipv4_addr
    elements = { "vif8.0" . 10.137.0.10 }
  }

  chain prerouting {
    type filter hook prerouting priority raw; policy accept;
    iifgroup 2 goto antispoof
    ip saddr @downstream counter packets 0 bytes 0 drop
  }

  chain antispoof {
    iifname . ip saddr @allowed accept
    counter packets 0 bytes 0 drop
  }

  chain postrouting {
    type nat hook postrouting priority srcnat; policy accept;
    oifgroup 2 accept
    oif "lo" accept
    masquerade
  }

  chain input {
    type filter hook input priority filter; policy drop;
    jump custom-input
  }
}
```



---

[apparatus](#) 26 April 7, 2024, 11:10am

darkgh05t:

```
chain nat {
    type nat hook prerouting priority dstnat; policy accept;
    iifname "vif*" tcp dport 53 dnat to 10.64.0.1
    iifname "vif*" udp dport 53 dnat to 10.64.0.1
}

chain dnat-dns {
    type nat hook prerouting priority dstnat; policy accept;
    ip daddr 10.139.1.1 udp dport 53 dnat to 10.139.1.1
    ip daddr 10.139.1.1 tcp dport 53 dnat to 10.139.1.1
    ip daddr 10.139.1.2 udp dport 53 dnat to 10.139.1.2
    ip daddr 10.139.1.2 tcp dport 53 dnat to 10.139.1.2
}
```

I'm not sure which rules will take priority here.

Can you change:

```
nft add chain qubes nat { type nat hook prerouting priority dstnat\; }
```

to

```
nft add chain qubes nat { type nat hook prerouting priority dstnat -1\; }
```

In your /rw/config/qubes-firewall-user-script and restart VPN qube?

1 Like

---

[darkgh05t](#) 27 April 7, 2024, 11:25am

just changed it and restarted qube, still no change.

---

[apparatus](#) 28 April 7, 2024, 11:31am

What if you replace 10.64.0.1 with 9.9.9.9?

You can run these commands for a test in your VPN qube:

```
sudo nft flush chain ip qubes nat
sudo nft add rule qubes nat iifname == "vif*" tcp dport 53 dnat 9.9.9.9
sudo nft add rule qubes nat iifname == "vif*" udp dport 53 dnat 9.9.9.9
```

1 Like

---

[darkgh05t](#) 29 April 7, 2024, 11:43am

just ran these commands and still no connection on the appvm,

---

[apparatus](#) 30 April 7, 2024, 12:06pm

Can you check if curl with IP address will work in AppVM?

```
curl https://9.9.9.9
```

---

[darkgh05t](#) 31 April 7, 2024, 12:12pm

```
[user@work ~]$ curl https://9.9.9.9
not found[user@work ~]$
```

---

[apparatus](#) 32 April 7, 2024, 12:14pm

Ok, seems to really be a problem with DNS.  
Does DNS work in VPN qube itself?

---

[solene](#) 33 April 7, 2024, 12:19pm

Could you try to modify the fix DNS part by adding the keyword counter at the end, do some DNS requests in an appvm and then use `nft list ruleset` (this will show all rules in the mullvad vpn qube, if you added firewall rules in an appvm, it will be displayed, this may leak information you don't want to)

this should look like this

```
DNS=10.64.0.1
nft add chain qubes nat { type nat hook prerouting priority dstnat\; }
nft add rule qubes nat iifname == "vif*" tcp dport 53 dnat "$DNS" counter
nft add rule qubes nat iifname == "vif*" udp dport 53 dnat "$DNS" counter
```

we will be able to figure if the rules is actually used

---

[darkgh05t](#) 34 April 7, 2024, 12:20pm

yeah it works fine in the VPN qube, for some reason i just cant get the appvm to connect to it, the browsers wont connect.

---

[apparatus](#) 35 April 7, 2024, 12:24pm

What's the content of `/etc/resolv.conf` in AppVM?

---

[solene](#) 36 April 7, 2024, 1:32pm

this shouldn't matter because the mullvad qube intercept it and redirect using nftables

---

[apparatus](#) 37 April 7, 2024, 1:34pm

It could be empty.

1 Like

---

[darkgh05t](#) 38 April 8, 2024, 4:19am

```
[user@work ~]$ sudo nft list ruleset
table ip qubes {
set downstream {
type ipv4_addr
}

set allowed {
    type ifname . ipv4_addr
}

chain prerouting {
    type filter hook prerouting priority raw; policy accept;
    iifgroup 2 goto antispoof
    ip saddr @downstream counter packets 0 bytes 0 drop
}

chain antispoof {
    iifname . ip saddr @allowed accept
    counter packets 0 bytes 0 drop
}

chain postrouting {
    type nat hook postrouting priority srcnat; policy accept;
    oifgroup 2 accept
    oif "lo" accept
    masquerade
}

chain input {
    type filter hook input priority filter; policy drop;
    jump custom-input
    ct state invalid counter packets 0 bytes 0 drop
}
}
table ip6 qubes {
set downstream {
type ipv6_addr
}

set allowed {
    type ifname . ipv6_addr
}

chain antispoof {
    iifname . ip6 saddr @allowed accept
    counter packets 0 bytes 0 drop
}

chain prerouting {
    type filter hook prerouting priority raw; policy accept;
```

```

    iifgroup 2 goto antispoof
    ip6 saddr @downstream counter packets 0 bytes 0 drop
}

chain postrouting {
    type nat hook postrouting priority srcnat; policy accept;
    oifgroup 2 accept
    oif "lo" accept
    masquerade
}

chain _icmpv6 {
    meta l4proto != ipv6-icmp counter packets 0 bytes 0 reject with icmpv6 admin-prohibited
    icmpv6 type { nd-router-advert, nd-redirect } counter packets 0 bytes 0 drop
    accept
}

[user@work ~]$

```

---

[darkgh05t](#) 39 April 8, 2024, 4:21am

```

nameserver 10.139.1.1
nameserver 10.139.1.2

```

---

[apparatus](#) 40 April 8, 2024, 4:26am

Do some DNS requests in an appvm and then use `sudo nft list chain ip qubes nat` in your VPN qube to check the counter.

---

[darkgh05t](#) 41 April 8, 2024, 4:37am

```

[user@sys-vpn ~]$ sudo nft list chain ip qubes nat
table ip qubes {
chain nat {
type nat hook prerouting priority dstnat; policy accept;
iifname "vif*" tcp dport 53 dnat to 10.64.0.1
iifname "vif*" udp dport 53 dnat to 10.64.0.1
}
}
[user@sys-vpn ~]$

```

This is what i get in the VPN Qube

---

[apparatus](#) 42 April 8, 2024, 4:39am

Did you add counter to the rules in VPN qube?

solene:

```

DNS=10.64.0.1
nft add chain qubes nat { type nat hook prerouting priority dstnat\; }

```

```
nft add rule qubes nat iifname == "vif*" tcp dport 53 dnat "$DNS" counter
nft add rule qubes nat iifname == "vif*" udp dport 53 dnat "$DNS" counter
```

---

[darkgh05t](#) 43 April 8, 2024, 4:41am

Yes this is what i have currently

DNS=10.64.0.1

```
nft add chain qubes nat { type nat hook prerouting priority dstnat; }
nft add rule qubes nat iifname == "vif*" tcp dport 53 dnat "$DNS" counter
nft add rule qubes nat iifname == "vif*" udp dport 53 dnat "$DNS" counter
nft add rule ip qubes custom-forward tcp flags syn / syn,rst tcp option maxseg size set rt mtu
nft add rule qubes custom-forward oifname eth0 counter drop
nft add rule ip6 qubes custom-forward oifname eth0 counter drop
```

---

[apparatus](#) 44 April 8, 2024, 4:45am

There was an error, counter was in the wrong place.  
These ones are right:

```
DNS=10.64.0.1
nft add chain qubes nat { type nat hook prerouting priority dstnat\; }
nft add rule qubes nat iifname == "vif*" tcp dport 53 counter dnat "$DNS"
nft add rule qubes nat iifname == "vif*" udp dport 53 counter dnat "$DNS"
```

---

[darkgh05t](#) 45 April 8, 2024, 4:52am

```
ok i fixed up the script, and run
[user@sys-vpn ~]$ sudo nft list chain ip qubes nat
table ip qubes {
chain nat {
type nat hook prerouting priority dstnat; policy accept;
iifname "vif*" tcp dport 53 counter packets 0 bytes 0 dnat to 10.64.0.1
iifname "vif*" udp dport 53 counter packets 0 bytes 0 dnat to 10.64.0.1
}
}
[user@sys-vpn ~]$
```

---

[apparatus](#) 46 April 8, 2024, 4:53am

Try to make some DNS requests in your AppVM connected to this VPN qube.  
Like open some site or ping quad9.net.  
Then check the counter.

---

[darkgh05t](#) 47 April 8, 2024, 4:55am

yes i did that running ping 9.9.9.9 and [quad9.net](#) and also tried to load a page on the browser, while running the

script, same results 0 bytes ?

---

[apparatus](#) 48 April 8, 2024, 4:56am

What's the output of this command in dom0?

```
qvm-firewall qubename
```

Change qubename to the name of your AppVM where you're testing the connection.

---

[apparatus](#) 49 April 8, 2024, 4:59am

Also change:

```
nft add chain qubes nat { type nat hook prerouting priority dstnat\; }
```

to

```
nft add chain qubes nat { type nat hook prerouting priority dstnat -1\; }
```

And try again after VPN qube restart.

---

[darkgh05t](#) 50 April 8, 2024, 5:11am

```
[axe@dom0 ~]$ qvm-firewall work  
NO ACTION HOST PROTOCOL PORT(S) SPECIAL TARGET  
0 accept - - - - -  
[axe@dom0 ~]$
```

Sory couldnt copy past this one, but this is pretty much the output

---

[darkgh05t](#) 51 April 8, 2024, 5:11am

yes just changed this but still not working

---

[apparatus](#) 52 April 8, 2024, 5:30am

darkgh05t:

Sory couldnt copy past this one, but this is pretty much the output

Just FYI, you can copy dom0 clipboard like this:

### [How to copy from dom0](#)

This page covers copying files and clipboard text between dom0 and domUs. Since dom0 is special, the processes are different from copying and pasting text between qubes and copying and moving files between



Run these commands in your work qube for a test:

```
echo 'nameserver 9.9.9.9' > /etc/resolv.conf
ping -c 2 9.9.9.9
ping -c 2 quad9.net
```

And what's the output of this command in dom0?

```
qvm-firewall vpnqubename
```

Change vpnqubename to the name of your VPN qube.

---

[darkgh05t](#) 53 April 8, 2024, 5:39am

ok here is the results in the work qube

```
[user@work ~]$ echo 'nameserver 9.9.9.9' > /etc/resolv.conf
ping -c 2 9.9.9.9
ping -c 2 quad9.net
bash: /etc/resolv.conf: Permission denied
PING 9.9.9.9 (9.9.9.9) 56(84) bytes of data.
64 bytes from 9.9.9.9: icmp_seq=1 ttl=58 time=31.5 ms
64 bytes from 9.9.9.9: icmp_seq=2 ttl=58 time=26.6 ms

— 9.9.9.9 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 26.576/29.052/31.529/2.476 ms
ping: quad9.net: Temporary failure in name resolution
[user@work ~]$
```

and in the dom0 im getting the same empty results after running qvm-firewall sys-vpn

```
[axe@dom0 ~]$ qvm-firewall sys-vpn
NO ACTION HOST PROTOCOL PORT(S) SPECIAL TARGET ICMP TYPE EXPIRE COMMENT
0 accept -----
[axe@dom0 ~]$
```

---

[apparatus](#) 54 April 8, 2024, 5:46am

You need to add sudo, I forgot about it, check these command again:

```
echo 'nameserver 9.9.9.9' | sudo tee /etc/resolv.conf
ping -c 2 9.9.9.9
ping -c 2 quad9.net
```

---

[darkgh05t](#) 55 April 8, 2024, 5:50am

```
[user@work ~]$ echo 'nameserver 9.9.9.9' | sudo tee /etc/resolv.conf
```

```
ping -c 2 9.9.9.9
ping -c 2 quad9.net
nameserver 9.9.9.9
PING 9.9.9.9 (9.9.9.9) 56(84) bytes of data.
64 bytes from 9.9.9.9: icmp_seq=1 ttl=58 time=26.6 ms
64 bytes from 9.9.9.9: icmp_seq=2 ttl=58 time=26.5 ms

— 9.9.9.9 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 26.511/26.538/26.565/0.027 ms
ping: quad9.net: Temporary failure in name resolution
[user@work ~]$
```

And still no change in dom0

---

[apparatus](#) 56 April 8, 2024, 6:05am

Can you run these commands in VPN qube:

```
sudo nft flush chain ip qubes nat
sudo nft flush chain ip qubes dnat-dns
```

And try to run these commands in your work qube?

```
echo 'nameserver 9.9.9.9' | sudo tee /etc/resolv.conf
ping -c 1 quad9.net
```

---

[darkgh05t](#) 57 April 8, 2024, 6:11am

here are the results in the work qube

```
[user@work ~]$ echo 'nameserver 9.9.9.9' | sudo tee /etc/resolv.conf
ping -c 1 quad9.net
nameserver 9.9.9.9
ping: quad9.net: Temporary failure in name resolution
[user@work ~]$
```

---

[apparatus](#) 58 April 8, 2024, 6:18am

Restart VPN qube and then run this command in VPN qube:

```
sudo nft chain ip qubes forward '{ policy accept ; }'
```

Then run this command in your work qube:

```
ping -c 1 quad9.net
```

---

[darkgh05t](#) 59 April 8, 2024, 6:34am

ok did those steps.



and this is still the result in the work qube

```
[user@work ~]$ ping -c 1 quad9.net
ping: quad9.net: Temporary failure in name resolution
[user@work ~]$
```

---

[apparatus](#) 60 April 8, 2024, 7:02am

Run this command in VPN qube:

```
sudo nft insert rule qubes custom-forward log
```

Then run this command in VPN qube to view the firewall logs:

```
sudo journalctl -f
```

And then run this command in your work qube:

```
ping -c 1 quad9.net
```

What's the output of the journalctl command in VPN qube after the ping?

---

[darkgh05t](#) 61 April 8, 2024, 7:10am

ok the last line on this log happened after the ping on the work qube

```
[user@sys-vpn ~]$ sudo journalctl -f
Apr 08 17:05:26 sys-vpn sudo[1564]: user : TTY=pts/0 ; PWD=/home/user ; USER=root ; COMMAND=/usr/bin/journalctl
-f
Apr 08 17:05:26 sys-vpn audit[1564]: CRED_REFR pid=1564 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred
grantors=pam_env,pam_localuser,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0
res=success'
Apr 08 17:05:26 sys-vpn kernel: audit: type=1101 audit(1712559926.528:163): pid=1564 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting
grantors=pam_unix,pam_localuser acct="user" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0
res=success'
Apr 08 17:05:26 sys-vpn kernel: audit: type=1123 audit(1712559926.528:164): pid=1564 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/user"
cmd=6A6F75726E616C63746C202D66 exe="/usr/bin/sudo" terminal=pts/0 res=success'
Apr 08 17:05:26 sys-vpn kernel: audit: type=1110 audit(1712559926.529:165): pid=1564 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred
grantors=pam_env,pam_localuser,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0
res=success'
Apr 08 17:05:26 sys-vpn sudo[1564]: pam_unix(sudo:session): session opened for user root(uid=0) by user(uid=1000)
Apr 08 17:05:26 sys-vpn audit[1564]: USER_START pid=1564 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open
grantors=pam_keyinit,pam_limits,pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo"
hostname=? addr=? terminal=/dev/pts/0 res=success'
Apr 08 17:05:26 sys-vpn kernel: audit: type=1105 audit(1712559926.532:166): pid=1564 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open
grantors=pam_keyinit,pam_limits,pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo"
hostname=? addr=? terminal=/dev/pts/0 res=success'
Apr 08 17:05:26 sys-vpn audit[1565]: USER_ROLE_CHANGE pid=1565 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='newrole: old-
```

```
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 new-
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 exe="/usr/bin/sudo" hostname=? addr=? terminal=/
dev/pts/1 res=success'
Apr 08 17:05:26 sys-vpn kernel: audit: type=2300 audit(1712559926.533:167): pid=1565 uid=1000 auid=1000 ses=2
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='newrole: old-
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 new-
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 exe="/usr/bin/sudo" hostname=? addr=? terminal=/
dev/pts/1 res=success'
Apr 08 17:09:06 sys-vpn systemd[763]: Started dbus-1.3-org.xfce.Xfconf@1.service.
```

---

[apparatus](#) 62 April 8, 2024, 8:06am

Seems like nothing is coming from your work qube to sys-vpn qube.  
Just to make sure, are you sure that your work qube has sys-vpn as Net qube in its Qube Settings?  
Try to ping 9.9.9.9 from your work qube while looking at the firewall logs with journalctl.

---

[darkgh05t](#) 63 April 8, 2024, 8:22am

yup its definitely connected to sys-vpn, pinging 9.9.9.9 works fine but the ping [quad9.net](#) does not work. here are the log results from the ping 9.9.9.9

```
Apr 08 18:19:40 sys-vpn kernel: IN=vif12.0 OUT=wg0-mullvad MAC=fe:ff:ff:ff:ff:00:16:3e:5e:6c:00:08:00
SRC=10.137.0.10 DST=9.9.9.9 LEN=84 TOS=0x00 PREC=0x00 TTL=63 ID=12598 DF PROTO=ICMP TYPE=8 CODE=0 ID=1
SEQ=33
Apr 08 18:19:40 sys-vpn kernel: IN=wg0-mullvad OUT=vif12.0 MAC= SRC=9.9.9.9 DST=10.137.0.10 LEN=84 TOS=0x00
PREC=0x00 TTL=58 ID=10296 PROTO=ICMP TYPE=0 CODE=0 ID=1 SEQ=33
```

---

[apparatus](#) 64 April 8, 2024, 8:41am

Run these commands in sys-vpn:

```
sudo nft add chain ip qubes log-chain {type filter hook prerouting priority -450\;;}
sudo nft insert rule ip qubes log-chain log
```

Then start viewing the log in sys-vpn:

```
sudo journalctl -f -n0
```

And try to ping from your work qube:

```
ping -c 1 9.9.9.9
ping -c 1 quad9.net
```

---

[darkgh05t](#) 65 April 8, 2024, 8:47am

```
Apr 08 18:47:07 sys-vpn kernel: IN=vif12.0 OUT= MAC=fe:ff:ff:ff:ff:00:16:3e:5e:6c:00:08:00 SRC=10.137.0.10
DST=10.139.1.2 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=59884 DF PROTO=TCP SPT=57488 DPT=53 WINDOW=32120
RES=0x00 SYN URGP=0
Apr 08 18:47:08 sys-vpn kernel: IN=vif12.0 OUT= MAC=fe:ff:ff:ff:ff:00:16:3e:5e:6c:00:08:00 SRC=10.137.0.10
```

DST=10.139.1.1 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48024 DF PROTO=TCP SPT=60364 DPT=53 WINDOW=32120 RES=0x00 SYN URGP=0  
Apr 08 18:47:08 sys-vpn kernel: IN=vif12.0 OUT= MAC=fe:ff:ff:ff:ff:00:16:3e:5e:6c:00:08:00 SRC=10.137.0.10  
DST=10.139.1.2 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=59885 DF PROTO=TCP SPT=57488 DPT=53 WINDOW=32120 RES=0x00 SYN URGP=0  
Apr 08 18:47:09 sys-vpn kernel: IN=vif12.0 OUT= MAC=fe:ff:ff:ff:ff:00:16:3e:5e:6c:00:08:00 SRC=10.137.0.10  
DST=10.139.1.1 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48025 DF PROTO=TCP SPT=60364 DPT=53 WINDOW=32120 RES=0x00 SYN URGP=0

---

[apparatus](#) 66 April 8, 2024, 8:52am

What's the output of this command in sys-vpn?

```
sudo nft list ruleset
```

---

[darkgh05t](#) 67 April 8, 2024, 8:53am

```
[user@sys-vpn ~]$ sudo nft list ruleset
table ip qubes {
set downstream {
type ipv4_addr
elements = { 10.137.0.10 }
}

set allowed {
type ifname . ipv4_addr
elements = { "vif12.0" . 10.137.0.10 }
}

chain prerouting {
type filter hook prerouting priority raw; policy accept;
iifgroup 2 goto antispoof
ip saddr @downstream counter packets 0 bytes 0 drop
}

chain antispoof {
iifname . ip saddr @allowed accept
counter packets 0 bytes 0 drop
}

chain postrouting {
type nat hook postrouting priority srcnat; policy accept;
oifgroup 2 accept
oif "lo" accept
masquerade
}

chain input {
type filter hook input priority filter; policy drop;
jump custom-input
}
}
table ip6 qubes {
set downstream {
type ipv6_addr
}
```

```

set allowed {
    type ifname . ipv6_addr
}

chain antispooof {
    iifname . ip6 saddr @allowed accept
    counter packets 25 bytes 1612 drop
}

chain prerouting {
    type filter hook prerouting priority raw; policy accept;
    iifgroup 2 goto antispooof
    ip6 saddr @downstream counter packets 0 bytes 0 drop
}

chain postrouting {
    type nat hook postrouting priority srcnat; policy accept;
    oifgroup 2 accept
    oif "lo" accept
    masquerade
}

chain _icmpv6 {
    meta l4proto != ipv6-icmp counter packets 0 bytes 0 reject with icmpv6 admin-prohibited
    icmpv6 type { nd-router-advert, nd-redirect } counter packets 0 bytes 0 drop
    accept
}

}

table ip qubes-firewall {
chain forward {
type filter hook forward priority filter; policy drop;
ct state established,related accept
iifname != "vif*" accept
ip saddr 10.137.0.10 jump qbs-10-137-0-10
}

chain prerouting {
    type filter hook prerouting priority raw; policy accept;
    iifname != "vif*" ip saddr 10.137.0.10 drop
}

chain postrouting {
    type filter hook postrouting priority raw; policy accept;
    oifname != "vif*" ip daddr 10.137.0.10 drop
}

chain qbs-10-137-0-10 {
    accept
    reject with icmp admin-prohibited
}

}

table ip6 qubes-firewall {
chain forward {
type filter hook forward priority filter; policy drop;
ct state established,related accept
iifname != "vif*" accept
}

chain prerouting {

```

```

    type filter hook prerouting priority raw; policy accept;
}

chain postrouting {
    type filter hook postrouting priority raw; policy accept;
}

}

table inet mullvad {
chain prerouting {
type filter hook prerouting priority -199; policy accept;
iif != "wg0-mullvad" ct mark 0x00000f41 meta mark set 0x6d6f6c65
ip saddr 103.216.220.18 udp sport 21341 meta mark set 0x6d6f6c65
}

chain output {
    type filter hook output priority filter; policy drop;
    oif "lo" accept
    ct mark 0x00000f41 accept
    udp sport 68 ip daddr 255.255.255.255 udp dport 67 accept
    ip6 saddr fe80::/10 udp sport 546 ip6 daddr ff02::1:2 udp dport 547 accept
    ip6 saddr fe80::/10 udp sport 546 ip6 daddr ff05::1:3 udp dport 547 accept
    ip6 daddr ff02::2 icmpv6 type nd-router-solicit icmpv6 code no-route accept
    ip6 daddr ff02::1:ff00:0/104 icmpv6 type nd-neighbor-solicit icmpv6 code no-route accept
    ip6 daddr fe80::/10 icmpv6 type nd-neighbor-solicit icmpv6 code no-route accept
    ip6 daddr fe80::/10 icmpv6 type nd-neighbor-advert icmpv6 code no-route accept
    ip daddr 103.216.220.18 udp dport 21341 meta mark 0x6d6f6c65 accept
    oif "wg0-mullvad" udp dport 53 ip daddr 100.64.0.23 accept
    oif "wg0-mullvad" tcp dport 53 ip daddr 100.64.0.23 accept
    udp dport 53 reject
    tcp dport 53 reject with tcp reset
    oif "wg0-mullvad" accept
    reject
}

chain input {
    type filter hook input priority filter; policy drop;
    iif "lo" accept
    ct mark 0x00000f41 accept
    udp sport 67 udp dport 68 accept
    ip6 saddr fe80::/10 udp sport 547 ip6 daddr fe80::/10 udp dport 546 accept
}

table inet qubes-nat-accel {
flowtable qubes-accel {
hook ingress priority filter
devices = { eth0, lo, vif12.0 }
}

chain qubes-accel {
    type filter hook forward priority filter + 5; policy accept;
    meta l4proto { tcp, udp } iifgroup 2 oifgroup 1 flow add @qubes-accel
    counter packets 68 bytes 5712
}

}

[user@sys-vpn ~]$

```

Just to confirm, since I don't think you specified it, are you using Wireguard or OpenVPN in the app?

---

[darkgh05t](#) 69 April 8, 2024, 8:56am

using wireguard

---

[apparatus](#) 70 April 8, 2024, 8:57am

Run these commands in sys-vpn and check ping -c 1 quad9.net in your work qube:

```
sudo nft flush chain ip qubes nat
sudo nft add rule qubes nat iifname == "vif*" tcp dport 53 dnat 100.64.0.23
sudo nft add rule qubes nat iifname == "vif*" udp dport 53 dnat 100.64.0.23
```

---

[apparatus](#) 71 April 8, 2024, 8:59am

The mullvad app is creating the additional rules alongside the Qubes OS ones so they're conflicting if not set up properly.

The mullvad app is blocking all DNS queries except for the ones coming to the 100.64.0.23.

darkgh05t:

```
oif "wg0-mullvad" udp dport 53 ip daddr 100.64.0.23 accept
oif "wg0-mullvad" tcp dport 53 ip daddr 100.64.0.23 accept
udp dport 53 reject
tcp dport 53 reject with tcp reset
```

---

[darkgh05t](#) 72 April 8, 2024, 9:01am

apparatus:

ping -c 1 [quad9.net](#)

[user@work ~]\$ ping -c 1 9.9.9.9

ping -c 1 [quad9.net](#)

PING 9.9.9.9 (9.9.9.9) 56(84) bytes of data.

64 bytes from 9.9.9.9: icmp\_seq=1 ttl=58 time=28.6 ms

— 9.9.9.9 ping statistics —

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 28.641/28.641/28.641/0.000 ms

ping: [quad9.net](#): Temporary failure in name resolution

[user@work ~]\$ ping -c 1 [quad9.net](#)

PING [quad9.net](#) (216.21.3.77) 56(84) bytes of data.

64 bytes from [web1.sjc.rrdns.pch.net](#) (216.21.3.77): icmp\_seq=1 ttl=52 time=178 ms

— [quad9.net](#) ping statistics —

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 178.350/178.350/178.350/0.000 ms  
[user@work ~]\$

---

[apparatus](#) 73 April 8, 2024, 9:03am

Seems like it works, so just change the DNS to 100.64.0.23 in your /rw/config/qubes-firewall-user-script in sys-vpn.

---

[darkgh05t](#) 74 April 8, 2024, 9:03am

this changed something as now things are starting to work, abit laggy but browser is now starting to open

---

[DVM](#) 75 April 8, 2024, 9:05am

[@solene](#) The following script should be added to the main post. The DNS address will not always be 10.64.0.1, especially with OpenVPN and DNS filtering rules.

#### [Mullvad VPN App 4.2 setup guide](#)

Mullvad uses many different DNS addresses depending on what the user selects in the app. The default Wireguard DNS address is 10.64.0.1, but it can also be in the 100.64.0.x range if the user chooses to use the [DNS filtering rules](#). For OpenVPN, it's different too. Each port gives a different subnet and the DNS is always 10.x.0.1. DNS filtering (100.64.0.x) also works with OpenVPN. Since it's hard to know what protocol the user will be using and if they will be using any DNS filtering rules, I ...

---

[darkgh05t](#) 76 April 8, 2024, 9:08am

this did the job it works now, thank you for all the help. fantastic

---

[solene](#) 77 April 8, 2024, 9:10am

There is a much more elegant method for IVPN App but I couldn't get it to work with Mullvad which is weird, could you give it an eyeball?

```
systemctl restart systemd-resolved  
/usr/lib/qubes/qubes-setup-dnat-to-ns
```

When resolv.conf is overwritten, restarting systemd-resolved put it in "foreign mode" (where resolv.conf is managed by something else), and the qubes helper script should propagate the new DNS to the qubes properly

---

[solene](#) 78 April 8, 2024, 9:10am

congrats [@apparatus](#) et good job [@darkgh05t](#) 👍

---

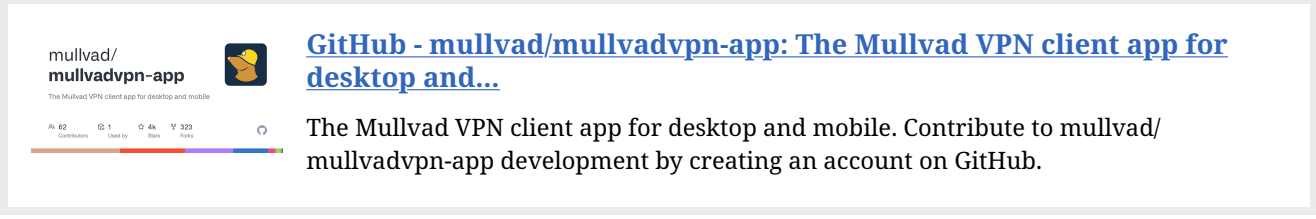
[darkgh05t](#) 79 April 8, 2024, 9:27am

ok i just noticed as i change the DNS filtering options in the app, we have issues connecting again. So adding this script should keep the DNS updated correct ?

---

[DVM](#) 80 April 8, 2024, 9:35am

The Mullvad App use multiple ways for their DNS customization (see TALPID\_DNS\_MODULE):



It always use “static-file” based on what I can see.

Your method might work on fedora, but systemd-resolved is not used on the debian template, so you would have to install it manually in that case.

Since it's easier to just follow what the application does by default, the script should work out of the box. If you want something more compact, you could just keep the `inotifywait` part and run `/usr/lib/qubes/qubes-setup-dnat -to-ns` every time the application edits the file.

---

[DVM](#) 81 April 8, 2024, 9:37am

Yes, the script will capture the DNS edited in `/etc/resolv.conf` and update the nftables rules.

---

[solene](#) 82 April 8, 2024, 9:38am

Could you edit the guide to make the change? 😊

---

[DVM](#) 83 April 8, 2024, 9:40am

Sure. Do you want me to put in the original script or do you want the more compact idea I talked about in my previous post?

---

[apparatus](#) 84 April 8, 2024, 9:46am

I think using `/usr/lib/qubes/qubes-setup-dnat -to-ns` is better in case Qubes OS will change something related to DNS handling in the future.

---

[solene](#) 85 April 8, 2024, 9:58am



I agree, using the Qubes OS scripts feels less hacky. The compact version would be better IMO 🤔

I wonder if this is required for Proton VPN as well, it should, right?

Actually, it would be nice if this “dns watch” was a qubes os service we could enable in the qube! I’ll fill a github issue to ask it as a request, and try to figure an implementation.

---

[DVM](#) 86 April 8, 2024, 10:42am

solene:

I agree, using the Qubes OS scripts feels less hacky. The compact version would be better IMO 🤔

I agree that this would be the best script to implement, but I’ve done some testing and while it works fine on Debian, it doesn’t on Fedora. qubes-setup-dnat-to-ns always uses systemd-resolved on Fedora, and only falls back to reading /etc/resolv.conf if it cannot reach the systemd service (which is why it works on Debian, since the service does not exist). This means that the DNS IP is not updated in the nftable dnat-dns chain when changing options in the application, which makes the script useless on Fedora. The original script works on both distributions, so even if it’s not the best, maybe it’s better to use it for now?

solene:

I wonder if this is required for Proton VPN as well, it should, right?

No idea, never used their app and if I remember correctly, they seem to rely on Network Manager anyway. So Qubes should update the IP with the VPN up/down event I guess.

solene:

Actually, it would be nice if this “dns watch” was a qubes os service we could enable in the qube! I’ll fill a github issue to ask it as a request, and try to figure an implementation.

That would be a good idea, yes. It would make a lot of services work out of the box.

---

[solene](#) 87 April 8, 2024, 10:45am

DVM:

No idea, never used their app and if I remember correctly, they seem to rely on Network Manager anyway. So Qubes should update the IP with the VPN up/down event I guess.

indeed, but Mullvad VPN app also create an entry in network manager IIRC

DVM:

The original script works on both distributions, so even if it’s not the best, maybe it’s better to use it for now?

sure, please go ahead 👍

---

[DVM](#) 88 April 8, 2024, 11:32am

solene:

indeed, but Mullvad VPN app also create an entry in network manager IIRC

Probably. They list “network-manager” as supported, but I don’t remember the app using it even when it was enabled.

solene:

sure, please go ahead 👍

It’s now available in the guide.

1 Like

---

[darkgh05t](#) 89 April 8, 2024, 12:37pm

Ok I just used this script and everything is working fine with fedora 39.

I tested with changing the dns filters in the app, then restarting the sys-vpn qube, everything works great now.

insert this script into /rw/config/rc.local

```
sudo systemctl restart systemd-resolved
sudo /usr/lib/qubes/qubes-setup-dnat-to-ns
```

1 Like

---

[solene](#) 90 April 8, 2024, 12:41pm

darkgh05t:

```
sudo systemctl restart systemd-resolved
sudo /usr/lib/qubes/qubes-setup-dnat-to-ns
```

you just added it and it works? great 🤔 you need to restart the qube when you make changes though, not sure if it’s a big deal for you.

---

[darkgh05t](#) 91 April 8, 2024, 12:49pm

yeah thats the only problem, I can live with that, but if the DNS could change on the fly without restarting the qube that would be great, it seems to only effect the DNS filtering in the app that you have to restart the qube,

---

[DVM](#) 92 April 8, 2024, 12:54pm

darkgh05t:

but if the DNS could change on the fly without restarting the qube that would be great

I have updated the guide with a script that does just that. Check out the “Fix DNS” part to get it.

---

[darkgh05t](#) 93 April 8, 2024, 12:59pm

ahh nice, i didnt see that. perfect thanks

---

[Whitecode](#) 94 May 4, 2024, 11:57pm

Did you manage to successfully install the mullvadapp into an appvm? I tried the guide you shared, but it didn't work. I also tried this

```
sudo mkdir -p /rw/config/qubes-bind-dirs.d
echo -e "binds+=( '/opt/mullvad-vpn' )" | sudo tee /rw/config/qubes-bind-
dirs.d/50_user.conf >/dev/null
```

---

[Dum0](#) 95 May 5, 2024, 6:54am

Thanks for this guide 😊

1 Like

---

[TommyTran732](#) 96 May 12, 2024, 11:52am

[@curbs94](#)

I updated the post on PrivSec: [Using Mullvad VPN on Qubes OS | PrivSec - A practical approach to Privacy and Security](#)

It uses systemd path now 😊

[@solene](#)

I think you might wanna switch to using a systemd path setup instead of inotify and rw/config/rc.local. It will be much cleaner 😊

3 Likes

---

[solene](#) 97 May 12, 2024, 12:06pm

TommyTran732:

I think you might wanna switch to using a systemd path setup instead of inotify and rw/config/rc.local. It will be much cleaner 😊

I didn't write that part, feel free to send an update 😊

---

[Whitecode](#) 98 May 16, 2024, 10:49pm

i created a mullvad app qube, but I have problems with the dns. The same problem that you have described in this guide. [ivpn guide](#) If you have time you can upload the section again for a mullvad qube? [@solene](#)

```
if ! grep "QUBES OS" /opt/ivpn/etc/firewall.sh >/dev/null
then
sudo sed -i '/-set_dns/a
#QUBES OS - specific operation
systemctl restart systemd-resolved || echo "Error: systemd-resolved"
/usr/lib/qubes/qubes-setup-dnat-to-ns || echo "Error: failed to run /usr/lib/qubes/qubes-setup-dnat-to-ns" /opt/ivpn/
etc/firewall.sh
fi
```

---

[solene](#) 99 May 17, 2024, 7:44am

Did you try the "[Fix DNS](#)" part of the guide?

---

[Whitecode](#) 100 May 17, 2024, 7:37pm

Yes it works very well now, but only until the MTU step. Just like the first attempt, after I finished the MTU step, I've got the dns problem again. As before the fix dns step. The app itself has an MTU setting. What is the value for this setting?

I also built a kill switch with the qvm firewall. Does it make sense in addition to qvm firewall to configure the kill switch?

---

[onoffonoff](#) 101 June 13, 2024, 3:21pm

has anyone taken the time to try this with a minimum template and know what are the least amount of packages needed for just running the gui client and acting as proxy?

---

[kowboybear](#) 102 August 16, 2024, 7:44am

Which firewall VM are you guys setting up qvm firewall rules in?

Is the proper setup

sys net->sys firewall → VPN qube → Another firewall qube → app vms

or

sys net → sys firewall → VPN qube → app vms.

The latter is the setup I'm currently using and it has worked for me. When I try the former setup with the extra firewall qube in front of the VPN connection, I end up having no internet in the app qube.

---

[apparatus](#) 103 August 16, 2024, 7:58am

If you want to limit VPN qube connections then you need to add the firewall rules to the VPN qube and both setups will work.

If you want to limit app vms connections then both setups will work as well, but this setup:

sys net->sys firewall → VPN qube → Another firewall qube → app vms

Will be more secure because the app vms firewall rules will be enforced in the Another firewall qube instead of a VPN qube in this setup:

sys net → sys firewall → VPN qube → app vms

If the VPN qube will be compromised (e.g. by VPN software) then the app vms firewall rules in it could be removed.

---

[solene](#) 104 August 16, 2024, 9:06am

kowboybear:

The latter is the setup im currently using and it has worked for me. when i try the former setup with the extra firewall qube in front of the vpn connection, i end up having no internet in the app qube.

Both should work, although as [@apparatus](#) said (and it is recommended in the official Qubes OS firewall documentation), a sys-firewall between the appvms and the vpn qube is recommended for security reasons

---

[glockmane](#) 105 September 1, 2024, 2:41pm

Sorry, am a bit confused, should i used the guide here, or the one on PrivSec or the one on the mullvad Page? I would prefer having the mullvad App and want to use the mullvad qube as Network for other cubes... Thank you very much 😊

---

[solene](#) 106 September 1, 2024, 2:55pm

well, it seems Mullvad updated their official guide to say iptables (the firewall command line tool) is not working anymore in Qubes OS 4.2, without updating their guide itself [Mullvad on Qubes OS 4](#)

the [PrivSec guide](#) is neat, but does not explain how to configure the VPN netvm to block everything (it's explaining here if you want). At least, it handles the /etc/resolv.conf issue better than this guide (I should update it to take the idea of a using a systemd unit)

---

[glockmane](#) 107 September 1, 2024, 4:28pm

You mean Killswitch Configuration?

---

[solene](#) 108 September 1, 2024, 8:21pm

Yes

---

[glockmane](#) 109 September 2, 2024, 3:59pm

Thanks, applied the nft lines to qubes-firewall-user-script in the template and wondered why it is not applied to the appvm, even not after creating a new appvm from the template, so I added them to the appvm too...

But I'm asking me what "Lockdown mode" in Mullvad app does, shouldn't it do the same? Is this not reliable? And should I still turn it on even after following your Killswitch method?

Thank you very much!

Here are some extensions.

## Debian minimal template

### Install dependencies

```
# [in dom0]
qvm-clone debian-12-minimal mullvad-vpn-app-d12m # or other name

# [in mullvad-vpn-app-d12m]
# netVM dependencies
apt install -y qubes-core-agent-networking qubes-core-agent-network-manager ntp
# Needed for Mullvad install script
apt install -y curl lsb-release
# Mullvad VPN app prerequisites
apt install -y libnss3 libasound2
# needed in order to listen for nameserver changes in /etc/resolv.conf
apt install inotify-tools
```

### Install Mullvad VPN app

```
# Download the Mullvad signing key
sudo curl -fsSL /usr/share/keyrings/mullvad-keyring.asc https://repository.mullvad.net/deb/

# Add the Mullvad repository server to apt
echo "deb [signed-by=/usr/share/keyrings/mullvad-keyring.asc arch=$( dpkg --print-architecture)] https://repository.mullvad.net/deb/ mullvad main" > /etc/apt/sources.list.d/mullvad.list

# Install the package
sudo apt update
sudo apt install mullvad-vpn
```

Original instructions can be found [here](#).

## DAITA

*Note: This is an experimental feature and currently supports only a few servers.*

DAITA (Defence against AI-guided Traffic Analysis) hides patterns in your encrypted VPN traffic. If anyone is monitoring your connection, this makes it significantly harder for them to identify what websites you are visiting. It does this by carefully adding network noise and making all network packets the same size. Attention: Since this increases your total network traffic, be cautious if you have a limited data plan. It can also negatively impact your network speed. Please consider this if you want to enable DAITA.

See [Defense against AI-guided Traffic Analysis \(DAITA\)](#) for mor infos. DAITA is supported with latest Linux beta version as of now, so we need to adjust the repository source (see [here](#)):

```
# add the Mullvad BETA repository server to apt
echo "deb [signed-by=/usr/share/keyrings/mullvad-keyring.asc arch=$( dpkg --print-architecture)] https://repository.mullvad.net/deb/ mullvad main" > /etc/apt/sources.list.d/mullvad.list
```

I haven't encountered any stability issues so far.

Then activate setting in Mullvad VPN app:

Settings → VPN settings → WireGuard settings → DAITA → **enable**

## Setup as ProxyVM / NetVM

Settings → VPN settings → Local network sharing → **enable**

This setting adds additional `nftables` entries, which are needed for Mullvad VPN app to work properly within NetVM as of now. I did not observe any other effects for local network access in context of Qubes OS, you also can inspect `nft` rules yourself. Credit goes to [privsec.dev](https://privsec.dev).

Of course you still need to forward DNS (`dnat`) as described in the guide, thanks [@DVM](#) for [the script](#).

## App-native killswitch / lockdown mode

Settings → VPN settings → Lockdown mode → **enable**

This is a more strict setting than “Kill switch” on same tab. It uses `nftables` to prevent leaks, hence not dependent on app startup; especially useful for people not used to invoke `nft` manually; seems to work well.

## Misc

Settings → VPN settings → Launch app on start-up → **enable** (for convenience)

2 Likes

---

[btrm](#) 111 September 3, 2024, 5:20pm

This guide seems not to work with latest Mullvad VPN and Qubes 4.2. I followed the instructions multiple times, but can't get VPN to work in my other cubes.

Net cube is set to `sys-firewall` (current) and the mullvad cube is using “`qubes-firewall`”. I also created the qube using the “provide network access to other qubes” in advanced settings.

No idea, what I'm missing here ...

---

[solene](#) 112 September 3, 2024, 6:16pm

btrm:

Net cube is set to `sys-firewall` (current)

by net qube, what do you mean?

btrm:

the mullvad cube is using “`qubes-firewall`”

this is right (it's a qube by the way)

btrm:

No idea, what I'm missing here ...

can you establish a VPN from the app? in a terminal in the mullvad qube, can you try

`ping -c 4 9.9.9.9` and if it works, try `ping -c 4 qubes-os.org`.

- If the first command does not work, there is something wrong, the VPN does not work.
- If the first one worked but not the second command, there is an issue with the DNS.
- If both commands work in mullvad qube, repeat in a qube using the mullvad VPN as a netvm.

My mullvad account for this guide expired so I can't verify myself if it still work.

---

[DAITA](#) 113 September 9, 2024, 9:05am

there are MTU Issues when using DAITA and quantum secure connections. Please update this guide.

---

[solene](#) 114 September 9, 2024, 12:39pm

Isn't the snippet about MTU problems enough to fix it?

---

[SimonSly](#) 115 September 15, 2024, 12:43pm

solene:

Add this to `/usr/local/bin/mullvad-dns.sh`

I seem to run into an issue at this point. For some reason there isn't this "mullvad-dns.sh" file in the `/user/local/bin/` folder. Have the context of the folder changed since recent mullvad update?

---

[solene](#) 116 September 15, 2024, 12:49pm

sorry, this was poor wording. I fixed it. You have to create the file with the provided content.

1 Like

---

[SimonSly](#) 117 September 15, 2024, 12:56pm

Thanks Solene, any chance you can show us n00bs how to create this type of file from the terminal im assuming?

Also how do we install this "inotify-tools" package, I tried the apt get command but it doesn't work.

Many thanks 😊

---

[solene](#) 118 September 16, 2024, 7:21am

SimonSly:

you can show us n00bs

be kind be yourself, consider yourself as a student or a learner 😊

SimonSly:

to create this type of file

Type `sudo nano /usr/local/bin/mullvad-dns.sh`, type the text and press "ctrl + x" to save. Then type `sudo chmod +x /usr/local/bin/mullvad-dns.sh` to make it executable.



SimonSly:

Also how do we install this “inotify-tools” package

if you are on fedora, it will be `sudo dnf install inotify-tools`, apt-get is for deb based distributions (ubuntu, debian, mint)

1 Like

---

[SimonSly](#) 119 September 16, 2024, 12:40pm

Thanks for everything Solene, works perfectly 😊

The only thing I didnt do was the killswitch as I didnt want to use Mullvad for all the qubes

---

[solene](#) 120 September 16, 2024, 12:42pm

SimonSly:

The only thing I didnt do was the killswitch as I didnt want to use Mullvad for all the qubes

if you want some qubes without mullvad, use sys-firewall as their netvm.

2 Likes

---

[glockmane](#) 121 September 17, 2024, 5:40pm

It's “nano” 😊

---

[solene](#) 122 September 17, 2024, 5:50pm

Thanks for reporting the typo 👍

---

[anon83904133](#) 123 September 24, 2024, 7:39pm

How can you update the qube? The normal update way for qubes always failes. Manually running `sudo dnf update && sudo dnf upgrade` returns something this:

```
Errors during downloading metadata for repository 'qubes-vm-r4.2-current':
- Curl error (6): Couldn't resolve host name for http://yum.qubesosfasa4z<i skip this part l
Error: Failed to download metadata for repo 'qubes-vm-r4.2-current': Cannot download rpomd.)
```

---

[trombon](#) 124 September 25, 2024, 4:26am

there are so many methods of installing VPN, wireguard, vpn app, networkmanager

can someone explain the underlying feature that makes the traffic go to VPN tunnel?

I understand it create wireguard interface for VPN, then traffic is sent there

how? does Linux firewall move traffic to VPN interface?

Some other setting in wireguard takes priority?

please explain!

---

[apparatus](#) 125 September 25, 2024, 5:35am

You're using onion repositories and they only work if you're updating through Tor.

If you want to update through VPN then change the repositories back to the clearnet ones.

---

[apparatus](#) 126 September 25, 2024, 5:38am

It's adding the default route through VPN interface with higher priority than the route through eth0 interface.

Read about routing in linux.

Check the output of these commands:

```
ip rule
ip route
ip route show table VPN_TABLE_NAME_OR_ID
```