Configuring a ProxyVM VPN Gateway

configuration, version-r41, template, security, networking

taradiddles 1 June 3, 2023, 12:42pm

This guide is not suitable for Qubes OS version 4.2 and later, see this post which contains a solution.

Note: If you seek to enhance your privacy, you may also wish to consider Whonix. You should also be aware of the potential risks of VPNs.

Although setting up a VPN connection is not by itself Qubes specific, Qubes includes a number of tools that can make the client-side setup of your VPN more versatile and secure. This document is a Qubes-specific outline for choosing the type of VM to use, and shows how to prepare a ProxyVM for either NetworkManager or a set of fail-safe VPN scripts.

Please refer to your guest OS and VPN service documentation when considering the specific steps and parameters for your connection(s); The relevant documentation for the Qubes default guest OS (Fedora) is Establishing a VPN Connection.

NetVM

The simplest case is to set up a VPN connection using the NetworkManager service inside your NetVM. Because the NetworkManager service is already started, you are ready to set up your VPN connection. However this has some disadvantages:

- You have to place (and probably save) your VPN credentials inside the NetVM, which is directly connected to the outside world
- All your AppVMs which are connected to the NetVM will be connected to the VPN (by default)

AppVM

While the NetworkManager service is not started here (for a good reason), you can configure any kind of VPN client in your AppVM as well. However this is only suggested if your VPN client has special requirements.

ProxyVM

One of the best unique features of Qubes OS is its special type of VM called a ProxyVM. The special thing is that your AppVMs see this as a NetVM (or uplink), and your NetVMs see it as a downstream AppVM. Because of this, you can place a ProxyVM between your AppVMs and your NetVM. This is how the default sys-firewall VM functions.

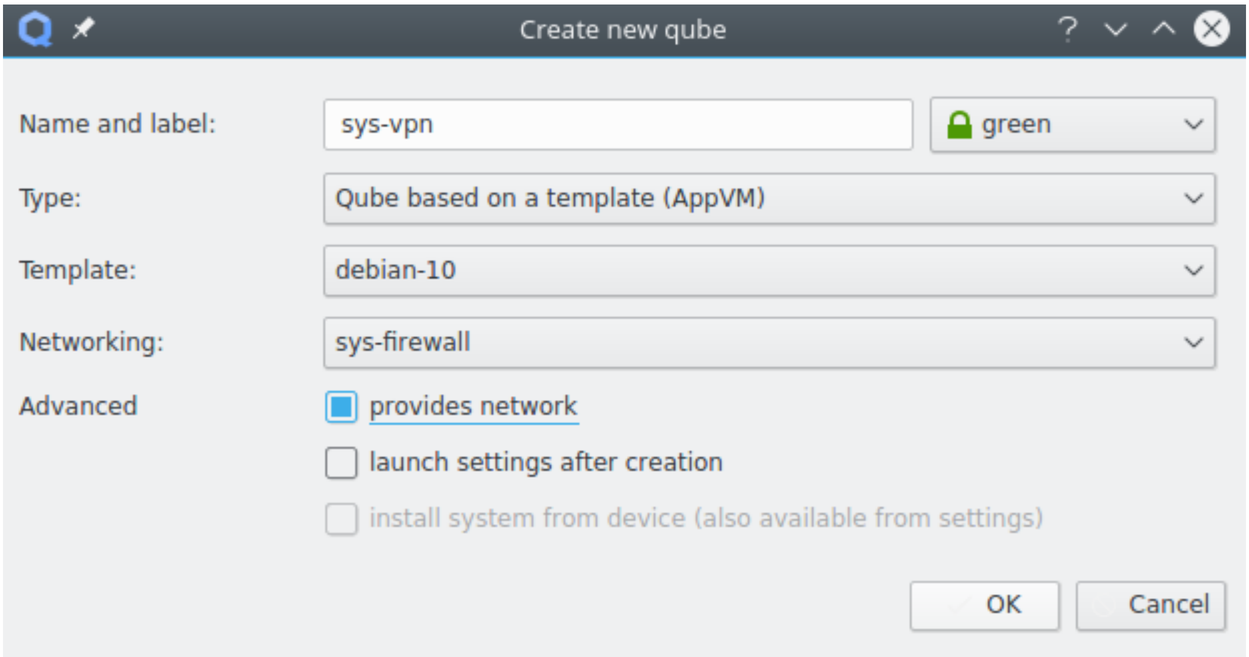
Using a ProxyVM to set up a VPN client gives you the ability to:

- Separate your VPN credentials from your NetVM.
- Separate your VPN credentials from your AppVM data.
- Easily control which of your AppVMs are connected to your VPN by simply setting it as a NetVM of the desired AppVM.

Set up a ProxyVM as a VPN gateway using

NetworkManager

1. Create a new VM, name it, click the ProxyVM radio button, and choose a color and template.



Create new qube

Name and label: sys-vpn green

Type: Qube based on a template (AppVM)

Template: debian-10

Networking: sys-firewall

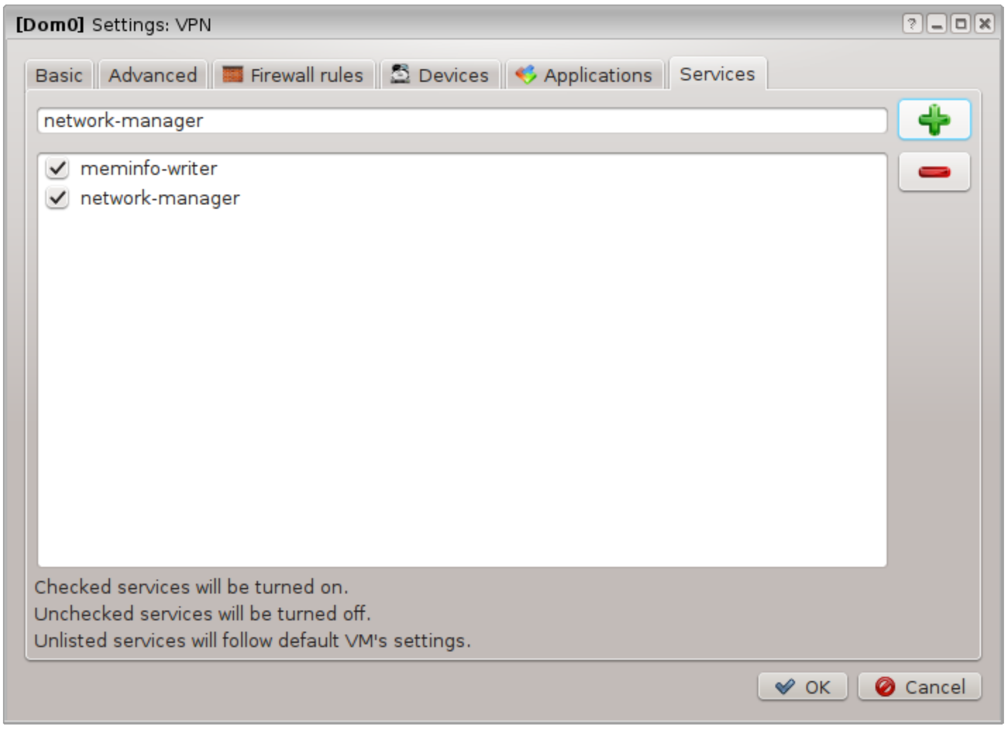
Advanced

☑ provides network

□ launch settings after creation

□ install system from device (also available from settings)

2. Add the `network-manager` service to this new VM.



[Dom0] Settings: VPN

network-manager

☑ meminfo-writer

☑ network-manager

Checked services will be turned on.
Unchecked services will be turned off.
Unlisted services will follow default VM's settings.

3. Set up your VPN as described in the NetworkManager documentation linked above.

4. (Optional) Make your VPN start automatically.

   Edit `/rw/config/rc.local` and add these lines:

```
# Automatically connect to the VPN once Internet is up
while ! ping -c 1 -W 1 1.1.1.1; do
   sleep 1
```

```
done
PWDFILE="/rw/config/NM-system-connections/secrets/passwd-file.txt"
nmcli connection up file-vpn-conn passwd-file $PWDFILE
```

You can find the actual “file-vpn-conn” in `/rw/config/NM-system-connections/`.

Create directory `/rw/config/NM-system-connections/secrets/` (You can put your `*.crt` and `*.pem` files here too). Create a new file `/rw/config/NM-system-connections/secrets/passwd-file.txt`:

```
vpn.secrets.password:XXXXXXXXXXXXXX
```

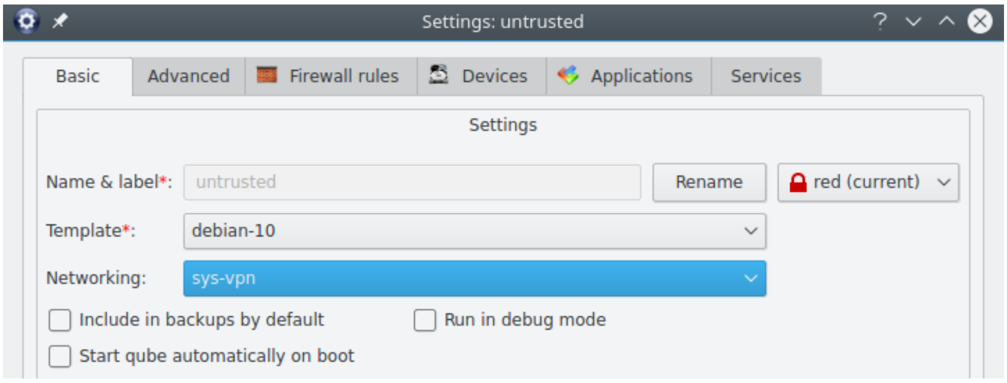
And substitute “XXXXXXXXXXXXXX” for the actual password. The contents of `passwd-file.txt` may differ depending on your VPN settings. See the **documentation for `nmcli up`**.

5. (Optional) Make the network fail-close for the AppVMs if the connection to the VPN breaks.

   Edit `/rw/config/qubes-firewall-user-script` and add these lines:

```
# Block forwarding of connections through upstream network device
# (in case the vpn tunnel breaks)
iptables -I FORWARD -o eth0 -j DROP
iptables -I FORWARD -i eth0 -j DROP
ip6tables -I FORWARD -o eth0 -j DROP
ip6tables -I FORWARD -i eth0 -j DROP
```

6. Configure your AppVMs to use the new VM as a NetVM.


Settings: untrusted

Settings

Name & label*: untrusted

red (current)

Template*: debian-10

Networking: sys-vpn

□ Include in backups by default

□ Run in debug mode

□ Start qube automatically on boot

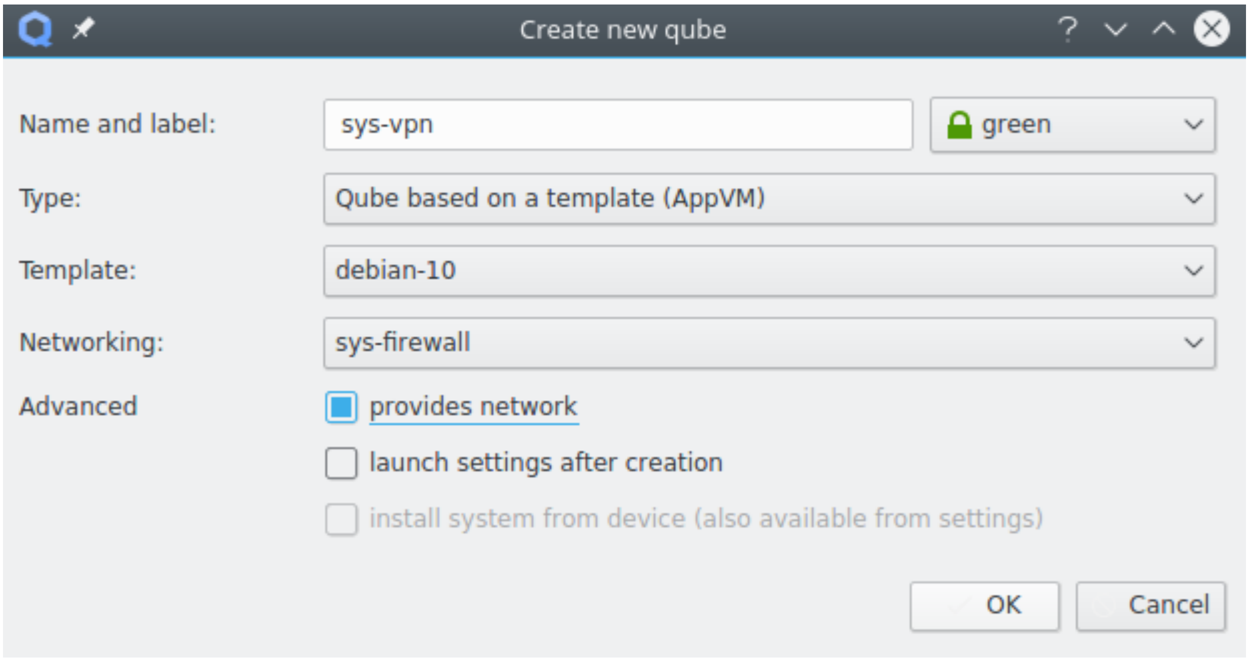
7. Optionally, you can install some **custom icons** for your VPN

Set up a ProxyVM as a VPN gateway using iptables and CLI scripts

This method is more involved than the one above, but has anti-leak features that also make the connection *fail closed* should it be interrupted. It has been tested with Fedora 30 and Debian 10 templates.

Before proceeding, you will need to download a copy of your VPN provider’s configuration file(s) and have your VPN login information handy.

1. Create a new VM, name it, choose “provides network”, and choose a color and template.



Name and label: sys-vpn | green

Type: Qube based on a template (AppVM)

Template: debian-10

Networking: sys-firewall

Advanced

☑ provides network

☐ launch settings after creation

☐ install system from device (also available from settings)

Note: Do not enable NetworkManager in the ProxyVM, as it can interfere with the scripts' DNS features. If you enabled NetworkManager or used other methods in a previous attempt, do not re-use the old ProxyVM… Create a new one according to this step.

If your choice of TemplateVM doesn't already have the VPN client software, you'll need to install the software in the template before proceeding. The 'openvpn' package comes installed in the Fedora template, and in Debian it can be installed with the following command:

```
sudo apt-get install openvpn
```

Disable any auto-starting service that comes with the software package. For example for OpenVPN.

```
sudo systemctl disable openvpn-server@.service
sudo systemctl disable openvpn-client@.service
```

2. Set up and test the VPN client. Make sure the VPN VM and its TemplateVM is not running. Run a terminal (CLI) in the VPN VM – this will start the VM. Then create a new `/rw/config/vpn` folder with:

```
sudo mkdir /rw/config/vpn
```

Copy your VPN configuration files to `/rw/config/vpn`. Your VPN config file should be named `openvpn-client.ovpn` so you can use the scripts below as is without modification. Otherwise you would have to replace the file name. Files accompanying the main config such as `*.crt` and `*.pem` should also be placed in the `/rw/config/vpn` folder.

Check or modify configuration file contents using a text editor:

```
sudo gedit /rw/config/vpn/openvpn-client.ovpn
```

Files referenced in `openvpn-client.ovpn` should not use absolute paths such as `/etc/...`.

The config should route all traffic through your VPN's interface after a connection is created;

For OpenVPN the directive for this is `redirect-gateway def1`.

Make sure it already includes or add:

```
redirect-gateway def1
```

The VPN client may not be able to prompt you for credentials when connecting to the server, so we'll add a reference to a file containing the VPN username and password. For example for OpenVPN, add or modify `auth-user-pass` like so:

```
auth-user-pass pass.txt
```

Save the `/rw/config/vpn/openvpn-client.ovpn` file.

Now make sure a `/rw/config/vpn/pass.txt` file actually exists.

```
sudo gedit /rw/config/vpn/pass.txt
```

Add:

```
username
password
```

Replace `username` and `password` with your actual username and password.

Test your client configuration: Run the client from a CLI prompt in the 'vpn' folder, preferably as root. For example:

```
sudo openvpn --cd /rw/config/vpn --config openvpn-client.ovpn
```

Watch for status messages that indicate whether the connection is successful and test from another VPN VM terminal window with `ping`.

```
ping 1.1.1.1
```

`ping` can be aborted by pressing the two keys `ctrl` + `c` at the same time. DNS may be tested at this point by replacing addresses in `/etc/resolv.conf` with ones appropriate for your VPN (although this file will not be used when setup is complete). Diagnose any connection problems using resources such as client documentation and help from your VPN service provider. Proceed to the next step when you're sure the basic VPN connection is working.

3. Create the DNS-handling script.

```
sudo gedit /rw/config/vpn/qubes-vpn-handler.sh
```

Add the following:

```
#!/bin/bash
set -e
export PATH="$PATH:/usr/sbin:/sbin"

```

```
case "$1" in

up)
# To override DHCP DNS, assign DNS addresses to 'vpn_dns' env variable befo
# Format is 'X.X.X.X  Y.Y.Y.Y [...]'
if [[ -z "$vpn_dns" ]] ; then
    # Parses DHCP foreign_option_* vars to automatically set DNS address tr
    for optionname in ${!foreign_option_*} ; do
        option="${!optionname}"
        unset fops; fops=($option)
        if [ ${fops[1]} == "DNS" ] ; then vpn_dns="$vpn_dns ${fops[2]}" ; f
    done
fi

iptables -t nat -F PR-QBS
if [[ -n "$vpn_dns" ]] ; then
    # Set DNS address translation in firewall:
    for addr in $vpn_dns; do
        iptables -t nat -A PR-QBS -i vif+ -p udp --dport 53 -j DNAT --to $a
        iptables -t nat -A PR-QBS -i vif+ -p tcp --dport 53 -j DNAT --to $a
    done
```

Save the script. Make it executable.

```
sudo chmod +x /rw/config/vpn/qubes-vpn-handler.sh
```

4. Configure client to use the DNS handling script. Using openvpn as an example, edit the config.

```
sudo gedit /rw/config/vpn/openvpn-client.ovpn
```

Add the following.

```
script-security 2
up 'qubes-vpn-handler.sh up'
down 'qubes-vpn-handler.sh down'
```

Remove other instances of lines starting with `script-security`, `up` or `down` should there be any others. Save the script. **Restart the client and test the connection again** ...this time from an AppVM!

5. Set up iptables anti-leak rules. Edit the firewall script.

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

Clear out the existing lines and add:

```
#!/bin/bash
#    Block forwarding of connections through upstream network device
#    (in case the vpn tunnel breaks):
iptables -I FORWARD -o eth0 -j DROP
iptables -I FORWARD -i eth0 -j DROP
ip6tables -I FORWARD -o eth0 -j DROP
```

```
ip6tables -I FORWARD -i eth0 -j DROP

#    Accept traffic to VPN
iptables -P OUTPUT ACCEPT
iptables -F OUTPUT

#    Add the `qvpn` group to system, if it doesn't already exist
if ! grep -q "^qvpn:" /etc/group ; then
     groupadd -rf qvpn
     sync
fi
sleep 2s

#    Block non-VPN traffic to clearnet
iptables -I OUTPUT -o eth0 -j DROP
#    Allow traffic from the `qvpn` group to the uplink interface (eth0);
#    Our VPN client will run with group `qvpn`.
iptables -I OUTPUT -p all -o eth0 -m owner --gid-owner qvpn -j ACCEPT
```

Save the script. Make it executable.

```
sudo chmod +x /rw/config/qubes-firewall-user-script
```

6. Set up the VPN’s autostart.

   ```
   sudo gedit /rw/config/rc.local
   ```

   Clear out the existing lines and add:

   ```
   #!/bin/bash
   VPN_CLIENT='openvpn'
   VPN_OPTIONS='--cd /rw/config/vpn/ --config openvpn-client.ovpn --daemon'

   groupadd -rf qvpn ; sleep 2s
   sg qvpn -c "$VPN_CLIENT $VPN_OPTIONS"
   su - -c 'notify-send "$(hostname): Starting $VPN_CLIENT..." --icon=network-
   ```

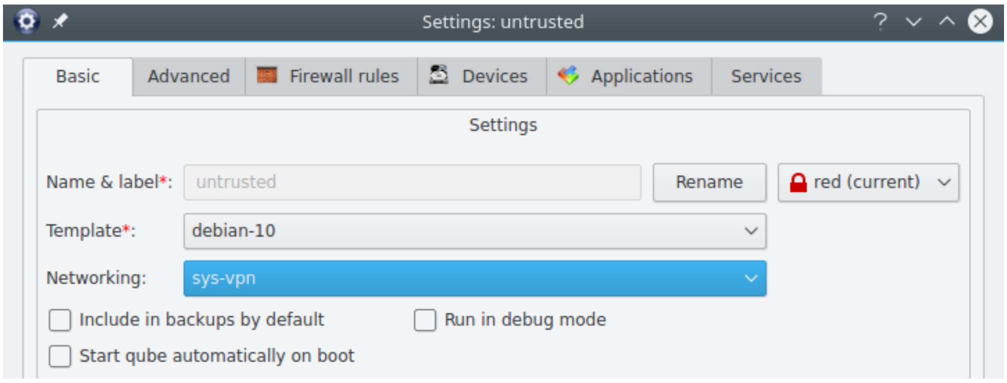
   If you are using anything other than OpenVPN, change the `VPN_CLIENT` and `VPN_OPTIONS` variables to match your VPN software. Save the script. Make it executable.

   ```
   sudo chmod +x /rw/config/rc.local
   ```

7. Restart the new VM! The link should then be established automatically with a popup notification to that effect.

Usage

Configure your AppVMs to use the VPN VM as a NetVM…



Settings: untrusted

Name & label*: untrusted — red (current)

Template*: debian-10

Networking: sys-vpn

□ Include in backups by default □ Run in debug mode

□ Start qube automatically on boot

If you want to update your TemplateVMs through the VPN, you can enable the `qubes-updates-proxy` service for your new VPN VM and configure the [qubes-rpc policy](#).

Troubleshooting

See the [VPN Troubleshooting](#) guide for tips on how to fix common VPN issues.

► This document was migrated from the qubes-community project
1 Like

[ProtonVPN, without using protonvpn app. (Qubes OS 4.2.0)](#)

[Transition from Qubes 4.1 to 4.2 switch nftables for non-technical users what to do?](#)

[I want to create proton vpn Qube](#)

[Need some help with setting up mullvad vpn](#)

[IP Address configuration?](#)

[[SOLVED] 4.2 broke my oVPN qubes: Connection refused (fd=3,code=111)](#)

[[SOLVED] 4.2 broke my oVPN qubes: Connection refused (fd=3,code=111)](#)

[How can i migrate my vpn-scripts from f38(iptables) f39(nftables)?](#)

[Disposable VPN qubes, similar to a firefox-dvm (disp1234)](#)

[I want to create proton vpn Qube](#)

[Whonix ws VM no DNS when NetVM is not sys-whonix](#)

[Sys-vpn extremly slow](#)

[etaz](#) 2 January 29, 2024, 5:14pm

In case anyone is interested in needed changes for Qubes OS **4.2** (`iptables` → `nftables`), the following did work for me:

```
# /rw/config/vpn/qubes-vpn-handler.sh
```

```
#...
nft flush chain ip qubes dnat-dns
if [[ -n "$vpn_dns" ]] ; then
    # Set DNS address translation in firewall:
    for addr in $vpn_dns; do
        nft add rule qubes dnat-dns iifname == "vif*" tcp dport 53 dnat "$add
        nft add rule qubes dnat-dns iifname == "vif*" udp dport 53 dnat "$add
```

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

nft add rule qubes custom-forward oifname eth0 counter drop
nft add rule ip6 qubes custom-forward oifname eth0 counter drop
nft add rule qubes custom-forward iifname eth0 counter drop
nft add rule ip6 qubes custom-forward iifname eth0 counter drop

#    Accept traffic to VPN
nft 'add chain qubes output { type filter hook output priority 0; policy acce

# ...

#    Block non-VPN traffic to clearnet
nft insert rule ip qubes output oifname eth0 counter drop
#    Allow traffic from the `qvpn` group to the uplink interface (eth0);
#    Our VPN client will run with group `qvpn`.
nft insert rule ip qubes output oifname eth0 skgid qvpn accept
```

You can also use `iptables-translate` to try out translation from one to the other.

Also to disable OpenVPN in Debian:

```
systemctl disable --now openvpn.service
```

5 Likes

---

mirome 3 February 5, 2024, 9:27am

Thx for the nft rules.
But I think there is a little issue there. The rules in nft need to have priority specified. If not, they get the priority depending on when they were created/evaluated. In the qubes-firewall-user-script the last rules are for blocking all eth0 traffic and then to allow vpn traffic. this two rules need to switch places:

```
#    Allow traffic from the `qvpn` group to the uplink interface (eth0);
#    Our VPN client will run with group `qvpn`.
nft add rule ip qubes output oifname eth0 skgid qvpn accept

#    Block non-VPN traffic to clearnet
nft add rule ip qubes output oifname eth0 counter drop
```

1 Like

---

etaz 4 February 5, 2024, 11:02am

@mirome Good catch - thanks! This was a typo, I accidently replaced `nft insert` by `nft add`.

I cannot edit post currently, will notify mods.

–

Update: Fixed **Configuring a ProxyVM VPN Gateway - #2 by etaz** to use `nft insert`. This also aligns with `iptables -I` of original guide post and should be equivalent to **Configuring a ProxyVM VPN Gateway - #3 by mirome**.

1 Like

---

stardustspaceship 5 February 10, 2024, 2:39pm

@etaz , thank you for your `nftables` update - it was one of my first questions when updating to 4.2. For the setup guides for

> taradiddles:
>
> Set up a ProxyVM as a VPN gateway using NetworkManager

or

> taradiddles:
>
> Set up a ProxyVM as a VPN gateway using iptables and CLI scripts

do they both need to make an update to `qubes-vpn-handler.sh`?

---

scallyob 6 February 11, 2024, 2:23am

Just found this update for 4.2, my openVPN connection has not been working since upgrading to

4.2. I tried the new `qubes-vpn-handler.sh` by @etaz , but getting the same results as I did with old version:

```
2024-02-10 18:17:45 OpenVPN 2.6.8 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZ
2024-02-10 18:17:45 library versions: OpenSSL 3.0.9 30 May 2023, LZO 2.10
2024-02-10 18:17:45 DCO version: N/A
2024-02-10 18:17:45 NOTE: the current --script-security setting may allow thi
2024-02-10 18:17:45 TCP/UDP: Preserving recently used remote address: [AF_INE
2024-02-10 18:17:45 Socket Buffers: R=[131072->131072] S=[16384->16384]
2024-02-10 18:17:45 Attempting to establish TCP connection with [AF_INET]999.
2024-02-10 18:17:45 TCP connection established with [AF_INET]999.999.999.99:4
2024-02-10 18:17:45 TCPv4_CLIENT link local: (not bound)
2024-02-10 18:17:45 TCPv4_CLIENT link remote: [AF_INET]999.999.999.99:443
2024-02-10 18:18:45 TLS Error: TLS key negotiation failed to occur within 60
2024-02-10 18:18:45 TLS Error: TLS handshake failed
2024-02-10 18:18:45 Fatal TLS error (check_tls_errors_co), restarting
2024-02-10 18:18:45 SIGUSR1[soft,tls-error] received, process restarting
2024-02-10 18:18:45 Restart pause, 1 second(s)
```

[SOLVED] 4.2 broke my oVPN qubes: Connection refused (fd=3,code=111)

---

etaz 7 February 12, 2024, 12:17pm

> stardustspaceship:
>
> do they both need to make an update to `qubes-vpn-handler.sh`?

Above commands are to be used in conjunction with the *second* alternative:

> taradiddles:
>
> Set up a ProxyVM as a VPN gateway using iptables and CLI scripts

Haven't tried the first alternative with NetworkManager, but it does not mention any steps involving `qubes-vpn-handler.sh`, so I guess you don't need that.

> scallyob:
>
> getting the same results as I did with old version:

Hm, hard to say with this log. Mine looks same till your `TLS Error: TLS key negotiation failed to occur within`. Have you tried the step-by-step approach in OP, which suggests intermediate validation steps?

stardustspaceship 8 February 14, 2024, 2:39am

I've confirmed that when using the `NetworkManager` approach, you only need to add the following lines to prevent traffic from qubes connected to the `netvm`:

> etaz:
>
> ```
> nft add rule qubes custom-forward oifname eth0 counter drop
> nft add rule ip6 qubes custom-forward oifname eth0 counter drop
> nft add rule qubes custom-forward iifname eth0 counter drop
> nft add rule ip6 qubes custom-forward iifname eth0 counter drop
> ```

This may be off-topic, but when I was testing this, I noticed that when I disconnect from the VPN, traffic from *within* the `netvm` is still allowed while traffic from a depending qube will be blocked. For example, from within the `netvm`, if I run `curl https://ip.me`, I will get the clearnet IP. If I run the same command in another qube connected to the `netvm` (i.e. an appvm), the request will timeout.

Can someone explain this or point me to docs/posts?

etaz 9 February 26, 2024, 8:55am

> stardustspaceship:
>
> I noticed that when I disconnect from the VPN, traffic from *within* the `netvm` is still allowed while traffic from a depending qube will be blocked.

I've not tested the network manager approach - but it seems OP is missing a kill switch / DNS leak protection *from within* that net qube?
Manual CLI approach effectively does `DROP` the `OUTPUT` (net qube → Inet) per default by:

```
#    Block non-VPN traffic to clearnet
nft insert rule ip qubes output oifname eth0 counter drop
#    Allow traffic from the `qvpn` group to the uplink interface (eth0);
#    Our VPN client will run with group `qvpn`.
nft insert rule ip qubes output oifname eth0 skgid qvpn accept
```

Have you tried to setup firewall rules for VPN endpoint + hardening as descripted in **Wireguard VPN setup**?

qubiq 10 March 14, 2024, 9:45am

> etaz:

```
# ...
```

Does this mean that all the rest of the code that is specified in the header of the topic should be here? Or does that mean everything else needs to be deleted? Or delete something certain and keep another? Excuse me, but not everyone here reads code as much as a human language. Could you please send the full contents of the file, as it should be?

---

etaz 11 March 15, 2024, 6:36am

> qubiq:
>
> Could you please send the full contents of the file, as it should be?

No problem, below is a copy/paste from my vpn qube.

► `/rw/config/vpn/qubes-vpn-handler.sh`

Note: I disabled auto-restart at the bottom.

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

Old commands are commented, hence you can compare changes by looking at the lines around. If you are not so proficient with this topic yet (also for ease of use), I probably just would use above linked Wirguard VPN guide. Also note, in terms of security it is better to use Qubes firewall for a killswitch instead of a firewall script within the vpn qube.

How can i migrate my vpn-scripts from f38(iptables) f39(nftables)?

DVM 12 March 15, 2024, 10:07am

Why do you create a new chain for your DNS forwarding rules? Qubes creates the `dnat-dns` chain by default when the qube provides network for others. It would be better to flush this chain and add the rules there instead.

1 Like

---

etaz 13 March 15, 2024, 6:39pm

IIRC I was inspired by the firewall docs suggesting to create custom dnat chain for each qube. But that is a different context and your suggestion definitely makes sense. Also to flush existing Qubes DNS NAT rules, which aren't needed for VPN. Thanks for mentioning `dnat-dns` is the new `PR-QBS`!

Will update `qubes-vpn-handler.sh` :

```
nft flush chain ip qubes dnat-dns
#nft add chain qubes nat { type nat hook prerouting priority dstnat\; }

#...

nft add rule qubes dnat-dns iifname == "vif*" tcp dport 53 dnat "$addr"
nft add rule qubes dnat-dns iifname == "vif*" udp dport 53 dnat "$addr"
#iptables -t nat -A PR-QBS -i vif+ -p udp --dport 53 -j DNAT --to $addr
#iptables -t nat -A PR-QBS -i vif+ -p tcp --dport 53 -j DNAT --to $addr
```

I think it also makes sense to polish `/rw/config/qubes-firewall-user-script` (but need to test):

```
nft 'add chain qubes output { type filter hook output priority 0; policy drop
#nft 'add chain qubes output { type filter hook output priority 0; policy acc
```

so that this line isn't needed:

```
#    Block non-VPN traffic to clearnet
#nft insert rule ip qubes output oifname eth0 counter drop
#iptables -I OUTPUT -o eth0 -j DROP
```

I keep those old comments for now, so the changes make sense for future readers.

Also when having tested in a Fedora netvm, I had issues with `notify-send` executed as `root` and needed to install `mate-notification-daemon`. That lines otherwise might be just commented.

Tezeria 14 March 16, 2024, 2:16pm

I've been asking myself a question for a while. Since the change from iptables to nftables,
I use the network manager rather than the "manual way" as described here and in the official documentation (I use it because I find it more convenient to change vpn servers via the network manager).
I'd like to know if using the network manager can cause more security problems than the "manual way" (knowing that I limit connections only to the IPs of the vpn as @solene does in her **tutorial,** whether with wireguard or openvpn).

---

solene 15 March 16, 2024, 3:25pm

I don't think NetworkManager is doing much more than the wireguard client interface.

It's easier to script the cli method as you can run commands on start / stop if it's useful for you.

etaz 16 March 16, 2024, 3:36pm

If asking me, it boils down to 1. choosing a type of VPN application 2. preventing leaks between VPN and clearnet.

For 1. the CLI approach in theory probably has less attack surface than NetworkManager and fits better with minimal templates. NetworkManager is more convenient.

For 2.: Imo you can omit all those `iptables` and `nftables` shenanigans and just use `qvm-firewall`. VPN gateway usually needs only one or couple fix VPN IPs. It also offers more security, if your VPN qube itself gets compromised.

It was a good learning expericene to do these things with `nft`, but I probably stick to NetworkManager + `qvm-firewall` as well.

Tezeria 17 March 16, 2024, 4:58pm

Thanks for your answers 🙂

> etaz:
>
> fits better with minimal templates.

I use minimal template with network-manager and all is easy ok 😉

---

qubiq 18 March 20, 2024, 7:16pm

> etaz:
>
> Also note, in terms of security it is better to use Qubes firewall for a killswitch instead of a firewall script within the vpn qube.

When I tried to use the built-in firewall, I was confused by this feature.

> How to setup OpenVPN + Fedora(AppVM) for OVPN
>
> In the firewall setup, there is the following note: [qubes] After setting the rule, qvm-firewall shows 'accept dns': [383985] Does this mean that this "firewall" doesn't work? And a dns leak occurs?

Do you understand what that means? And why are some DNS is accepted?
I don't fully understand this. Please explain

Whitecode 19 May 4, 2024, 12:42am

Unfortunately, that didn’t work with me. I did everything exactly as in the guide and i have problems with qubes-vpn-handler.sh. The only possibility I can successfully build the connection is if I remove the lines

up ‘qubes-vpn-handler.sh up’
down ‘qubes-vpn-handler.sh down’

from the VPN config file. But as soon as I insert the up/down lines back into the VPN config file, I get an error message when connecting, and the connection fails.

WARNING: Failed running command (–up/–down): could not execute external program
Exiting due fatal error

smlt 20 July 21, 2024, 12:19am

got the samething here bro… i used iptables-translate to convert all the iptables lines in scripts and got the same as you.

```
Error: syntax error, unexpected addr, expecting string
insert rule ip nat dnat-dns iifname vif* udp dport 53 counter dnat to $addr
                                                                       ^^^^
2024-07-20 20:12:22 WARNING: Failed running command (--up/--down): external p
2024-07-20 20:12:22 Exiting due to fatal error
```

some research in forum i find a user that has skills in nftables, the user is @solene , please could you help me fixing this error? thank you.

solene 21 July 21, 2024, 9:06am

> smlt:
>
> ```
> insert rule ip nat dnat-dns iifname vif* udp dport 53 counter dnat to $add
>                                                                        ^^^
> ```

it looks like you tried iptables-translate on a line with a variable, it doesn’t know what to do with `$addr`

smlt 22 July 21, 2024, 5:12pm

i made it work, but now the problem is i have connection inside the appvm–vpn but cant use it as proxy to another qube… **here is my topic**

---

annulet 23 July 31, 2024, 5:17pm

Regarding anti-leak rules:
In a netvm, I normally would have expected `FORWARD` rules instead of `OUTPUT`, as it basically is a router and forwards packets from a client qube to upstream.

Please confirm if following is right (thanks in advance!):
The OpenVPN client captures all traffic from all incoming network interfaces via

```
redirect-gateway def1
```

, so all relevant traffic belongs to OpenVPN client. And since OpenVPN is a local process, all network calls go through `OUTPUT`. NetworkManager analogue, but doesn’t need above change in `.ovpn` file. Seems it automatically grabs all incoming traffic and redirects it to VPN.

---

apparatus 24 August 1, 2024, 5:45am

With `redirect-gateway def1` all traffic is redirected to the VPN only if the openvpn is connected. If the VPN is disconnected then all the traffic originating from sys-vpn will go through clearnet.
These rules block all outgoing traffic to eth0 that is not originating from openvpn process:

> taradiddles:
>
> ```
> #    Accept traffic to VPN
> iptables -P OUTPUT ACCEPT
> iptables -F OUTPUT
>
> #    Add the `qvpn` group to system, if it doesn't already exist
> if ! grep -q "^qvpn:" /etc/group ; then
>      groupadd -rf qvpn
>      sync
> fi
> sleep 2s
>
> #    Block non-VPN traffic to clearnet
> iptables -I OUTPUT -o eth0 -j DROP
> #    Allow traffic from the `qvpn` group to the uplink interface (eth0);
> #    Our VPN client will run with group `qvpn`.
> iptables -I OUTPUT -p all -o eth0 -m owner --gid-owner qvpn -j ACCEPT
> ```

For example, if you have updates check enabled for your sys-vpn qube and the updates check will begin when VPN is connected, then VPN will disconnect during updates check and updates check will continue through clearnet this would be a leak.

2 Likes

---

annulet 25 August 1, 2024, 8:01am

Thanks @apparatus ! Your answer makes it very clear. Good point with the background updates.

Update: I think, implementing a killswitch for NetworkManager is easier by whitelisting the OpenVPN/Wireguard network interface:

```
nft insert rule ip qubes output oifname 'wg*' counter accept
```

(Otherwise NetworkManager would need to be started as `qvpn` user somehow.)

Here is what I am doing:

```
# block forward hook as default
nft 'add chain ip qubes forward { counter; policy drop; }'
nft insert rule ip qubes custom-forward counter drop

# block output hook as default
nft 'add chain ip qubes output { type filter hook output priority 0; counter;
nft insert rule ip qubes output counter drop

# allow establishing initial connection to VPN gateway (wireguard/udp)
nft insert rule ip qubes output ip daddr <VPN GATEWAY IP> udp dport <VPN GATE

# allow outgoing traffic through link wg*
nft insert rule ip qubes output oifname 'wg*' counter accept
```

This assumes, there is one active WG connection at a time.

---

annulet 26 August 1, 2024, 6:05pm

Hm there is one thing left, I don't understand: Fully blocking all `forward` connections does not work. I could ping `1.1.1.1` from within `sys-vpn`, but not from client qube.

Instead of

```
# block forward hook as default
nft 'add chain ip qubes forward { counter; policy drop; }'
nft insert rule ip qubes custom-forward counter drop
```

, I needed to write:

```
nft insert rule ip qubes custom-forward oifname eth0 counter drop
```

and leave default `forward` policy `accept`ed to get pings from clients.

Is this some weirdness of the VPN client (NetworkManager, OpenVPN)?
It seems to intercept and redirect client qube traffic to tunnel interface `wg` at some point before the killswitch `eth0 drop` rule could kick in. But still `forward`ing seems needed. Not sure about the internals, how exactly traffic is re-routed by these programs…

(**tldr**) Never mind: VPN clients probably just change the default IP route (+ default DNS). So we get `wg` (or what it's named) instead of `eth0` as output interface in routine table. nfttables does the same thing as before, meaning packet still needs `accept` to be `forward`ed. `eth0` can be safely blacklisted, as not used during VPN session.

What confused me is that `ip route` entries are not changed, after NetworkManager has initiatiated VPN connection. I still see only the Qubes default gateway. Nameserver is changed though, looking at `/etc/resolv.conf`.

---

apparatus 27 August 9, 2024, 2:40pm

> annulet:
>
> (Otherwise NetworkManager would need to be started as `qvpn` user somehow.)

You can set the group in the OpenVPN config.
But it won't work for Wireguard.

> annulet:
>
> Here is what I am doing:
>
> ```
> # block forward hook as default
> nft 'add chain ip qubes forward { counter; policy drop; }'
> nft insert rule ip qubes custom-forward counter drop
>
> # block output hook as default
> nft 'add chain ip qubes output { type filter hook output priority 0; coun
> nft insert rule ip qubes output counter drop
>
> # allow establishing initial connection to VPN gateway (wireguard/udp)
> nft insert rule ip qubes output ip daddr <VPN GATEWAY IP> udp dport <VPN
>
> # allow outgoing traffic through link wg*
> nft insert rule ip qubes output oifname 'wg*' counter accept
> ```
>
> This assumes, there is one active WG connection at a time.

In some cases you may need to allow the output connections from `lo` and `vif+` interfaces.

> annulet:
>
> What confused me is that `ip route` entries are not changed, after NetworkManager has initiated VPN connection. I still see only the Qubes default gateway. Nameserver is changed though, looking at `/etc/resolv.conf`.

The Wireguard creates separate routing table.
You can show all tables with this command:

```
ip rule show
```

And check all routes in all tables using this command:

```
ip route show table all
```

---

heinzl 28 August 17, 2024, 10:33am

Hello,
I have several problems with the "iptables and CLI scripts method". On my other laptop with an older Qubes OS I have no problems get the VPN connection work but now I have the following:
I came until 4. and wanted to test the connection and started OpenVPN in the terminal. The process is stopped due to fatal error:

"qubes-vpn-handler.sh: line 19: iptables: command not found
2024-08-17 12:22:41 WARNING: Failed running command (–up/–down): could not execute external program
2024-08-17 12:22:41 Exiting due to fatal error"

I copied the code, why he cannot find "iptables"?

Thanks.

---

apparatus 29 August 17, 2024, 10:40am

The guide is for Qubes OS 4.1 so it's using iptables firewall.
In Qubes OS 4.2 the iptables firewall was replaced with nftables firewall.
To use this guide in Qubes OS 4.2 you need to replace the firewall rules from iptables to nftables in `/rw/config/vpn/qubes-vpn-handler.sh` and `/rw/config/qubes-firewall-user-script` files.
You can use the files from this post:

> **Configuring a ProxyVM VPN Gateway**
>
> No problem, below is a copy/paste from my vpn qube.

> ► `/rw/config/vpn/qubes-vpn-handler.sh`

---

heinzl 30 August 17, 2024, 3:13pm

Thank you very much for your help. After having some trouble it seems now to work but I have three more questions:

1. In the original qubes-firewall-user-script you can read:
"# This script is called at AppVM boot if this AppVM has the qubes-firewall

service enabled."

But in the guide I can read nothing about that. So, do I have to enable this service or not to prevent leaks?

2. After having some troubles and finally had no error messages anymore when openvpn is running, I tried in the VPN-qube to open a website via Firefox but it didn't work and there was only a blanket site and was loading all the time. As I stopped openvpn the website loaded with a TOR IP. BUT as I assign the VPN-qube to another AppVM, it worked and I reached a website with the VPN IP. Why is that, should I not also reach a website withing the VPN-qube with the vpn connection?

3. I would like to know, if it is possible to have multiple config files in the folder and make openvpn randomly use one everytime it starts?

Thanks again.

---

apparatus 31 August 17, 2024, 3:37pm

> heinzl:
>
> 1. In the original qubes-firewall-user-script you can read:
> "# This script is called at AppVM boot if this AppVM has the qubes-firewall
>
> # service enabled."
>
> But in the guide I can read nothing about that. So, do I have to enable this service or not to prevent leaks?

It's just a note for the users to understand in what cases is this file called.
You don't need to take any additional actions.

> heinzl:
>
> After having some troubles and finally had no error messages anymore when openvpn is running, I tried in the VPN-qube to open a website via Firefox but it didn't work and there was only a blanket site and was loading all the time. As I stopped openvpn the website loaded

> with a TOR IP. BUT as I assign the VPN-qube to another AppVM, it worked and I reached a website with the VPN IP. Why is that, should I not also reach a website withing the VPN-qube with the vpn connection?

Check your /etc/resolve.conf in VPN qube when you're connected to the VPN. Most probably is that your VPN qube is not using the DNS server provided by your VPN so the DNS resolution is not working in the VPN qube.

> heinzl:
>
> I would like to know, if it is possible to have multiple config files in the folder and make openvpn randomly use one everytime it starts?

Yes, just pick a random file from the group of files in the `/rw/config/rc.local` instead of `openvpn-client.ovpn` specifically.
Here is an example:

> **Wireguard VPN setup**
>
> Good news, with fedora-38 the network manager supports Wireguard out of the box! The only thing required are extra firewall rules in the VPN qube, as explained in **the community documentation about VPN**. What you'll need This guide assumes you are using a VPN service that has wireguard support, most of them do, but you can also add your own if you have a server. ℹ ProtonVPN has a free plan, it has limits but gives you a fully working VPN and they support WireGuard. This pro...

So you can do something like this:

```
VPN_CONF=$(ls /rw/config/vpn-configs-dir | sort -R | head -n 1)
VPN_OPTIONS='--cd /rw/config/vpn/ --config "vpn-configs-dir/$VPN_CONF" --daem
```

heinzl 32 August 17, 2024, 4:15pm

Thanks, but it seems to be for WireGuard?

"It's just a note for the users to understand in what cases is this file called.
You don't need to take any additional actions."

But I understand that like the code in there will not be executed if I don't enable the service so I do not have the leak protection?
I am asking my self anyways, why I can open a website with my clear IP if I edited the firewall-script?

apparatus 33 August 17, 2024, 4:43pm

> heinzl:
>
> Thanks, but it seems to be for WireGuard?

It doesn't matter, I'm just referring to the idea of using `| sort -R | head -n 1` commands on the list of the VPN config files.

> heinzl:
>
> But I understand that like the code in there will not be executed if I don't enable the service so I do not have the leak protection?

The `qubes-firewall` service is enabled by default for qubes that provides network for other qubes.

> heinzl:
>
> I am asking my self anyways, why I can open a website with my clear IP if I edited the firewall-script?

Describe in more details what do you mean. I didn't get your question.

---

heinzl 34 August 17, 2024, 6:37pm

Ok, it is a bit weird for me: I set up the anti-leak rules, then I restarted the VPN-qube (I forgot that before, so don't mind my question before) and if I then start openvpn manually, it doesn't work. I start openvpn and it says
"Could not determine IPv4/IPv6 protocol", "RESOLVE: Cannot resolve host address: XXXXXXX (Temporary failure in name resolution)", "Restart pause, 64 second(s)" and so on.
But if I start the VPN-qube with configured openvpn autostart, it worked and the link is up and I have the vpn ip with another AppVM. As soon as I kill openvpn and have no restart enabled, I can't start openvpn anymore, the terminal says that, what I wrote above. Why is that? If it is working on start-up then it should work too if I manually start openvpn with my config right?
And I am not able to get it working AFTER whonix only after sys-firewall. But for some cases I want both: VPN-TOR-VPN because some websites block TOR traffic.

Thank you again.

---

apparatus 35 August 18, 2024, 7:33am

> heinzl:
>
> Ok, it is a bit weird for me: I set up the anti-leak rules, then I restarted the VPN-qube (I forgot that before, so don't mind my question before) and if I then start openvpn manually, it doesn't work. I start openvpn and it says

> “Could not determine IPv4/IPv6 protocol”, “RESOLVE: Cannot resolve host address: XXXXXXX (Temporary failure in name resolution)”, “Restart pause, 64 second(s)” and so on.
> But if I start the VPN-qube with configured openvpn autostart, it worked and the link is up and I have the vpn ip with another AppVM. As soon as I kill openvpn and have no restart enabled, I can’t start openvpn anymore, the terminal says that, what I wrote above. Why is that? If it is working on start-up then it should work too if I manually start openvpn with my config right?

Did you run it as `qvpn` group?

```
sg qvpn -c "$VPN_CLIENT $VPN_OPTIONS"
```

The output traffic that is coming from other groups are blocked:

> etaz:
>
> ```
> #    Block non-VPN traffic to clearnet
> nft insert rule ip qubes output oifname eth0 counter drop
> ```

> heinzl:
>
> And I am not able to get it working AFTER whonix only after sys-firewall. But for some cases I want both: VPN-TOR-VPN because some websites block TOR traffic.

Do you use TCP or UDP to connect to your VPN?
Tor only works for TCP.

---

heinzl 36 August 18, 2024, 8:55am

> apparatus:
>
> Did you run it as `qvpn` group?
>
> ```
> sg qvpn -c "$VPN_CLIENT $VPN_OPTIONS"
> ```

I don’t know what you mean. I just made the scripts (with nft) and typed in the console while I am in the config folder: sudo openvpn --config CONFIG.ovpn. Then it hast these “resolve problems”. If I set up the autostart and restart the VPN-qube, it works. But then the same setting are used or not?

> apparatus:
>
> Do you use TCP or UDP to connect to your VPN?
> Tor only works for TCP.

I’m not sure, I didn’t change anything in that matter.
So I can’t one of my vpn configurations after TOR?

apparatus 37 August 18, 2024, 9:01am

> heinzl:
>
> I don’t know what you mean. I just made the scripts (with nft) and typed in the console while I am in the config folder: sudo openvpn --config CONFIG.ovpn. Then it hast these “resolve problems”. If I set up the autostart and restart the VPN-qube, it works. But then the same setting are used or not?

Run it like this:

```
sudo sg qvpn -c "openvpn --config CONFIG.ovpn"
```

> heinzl:
>
> I’m not sure, I didn’t change anything in that matter.
> So I can’t one of my vpn configurations after TOR?

What do you have in your openvpn config? `proto tcp` or `proto udp`?

heinzl 38 August 18, 2024, 10:59am

In the third line in the config there is
“proto udp”
Can I just add “tcp”?

For now I tried: VPN-Tor and if I make an IP check with the AppVM using sys-whonix as NetVM, I got an Tor ip. But I am not sure, if sys-whonix really uses sys-vpn - is it possible to check that he is using an vpn ip? In my understanding not, because Tor uses 3 relais and with an ip check I can only see the exit node right?

solene 39 August 18, 2024, 11:01am

yes you can use `proto tcp` if your VPN providers supports TCP on that port.

heinzl 40 August 18, 2024, 11:13am

Ok, I changed that to proto tcp and a vpn connection is etablished, but it still don’t work AFTER Tor. I can’t open a website if I using sys-whonix as NetVM for sys-vpn. Using sys-firewall as NetVM for sys-vpn, I can open a website.

apparatus 41 August 18, 2024, 12:11pm

> heinzl:
>
> For now I tried: VPN-Tor and if I make an IP check with the AppVM using sys-whonix as NetVM, I got an Tor ip. But I am not sure, if sys-whonix really uses sys-vpn - is it possible to check that he is using an vpn ip? In my understanding not, because Tor uses 3 relais and with an ip check I can only see the exit node right?

You can enable logging in sys-vpn firewall and check the logs:
https://wiki.nftables.org/wiki-nftables/index.php/Logging_traffic
Or enable rule counters to see how packets are going through sys-vpn.
Or use tcpdump to check the traffic.

> heinzl:
>
> Using sys-firewall as NetVM for sys-vpn, I can open a website.

Does it work with `proto tcp`?
Did you check that the IP to make sure that VPN is working?

heinzl 42 August 18, 2024, 3:35pm

Yes, if I using sys-firewall as NetVM for sys-vpn I opened a website for checking my ip and it was the vpn ip. That is working, But as soon as I give sys-whonix to sys-vpn as NetVM I can't open a website anymore, it's loading and loading.
And I have changed the line to "proto tcp" but it's still not working.

apparatus 43 August 18, 2024, 3:46pm

Did you try to restart sys-vpn after changing its net qube to sys-whonix?

heinzl 44 August 18, 2024, 3:57pm

Ok, after a reset I can open a website, the ip check tells me, it is the vpn ip. Thanks, thought I can change NetVMs on the fly via Qubes Manager.
But I am not sure if the sys-vpn "get it's net" from sys-whonix, if I type "curl https://ip.me" in the sys-vpn terminal I got "Could not resolve host: ip.me".

apparatus 45 August 18, 2024, 3:59pm

Run this command:

```
sudo sg qvpn -c "curl https://ip.me"
```

heinzl 46 August 18, 2024, 4:02pm

> apparatus:
>
> ```
> sudo sg qvpn -c "curl https://ip.me"
> ```

Inside the sys-vpn terminal right? Then I get the same answer.

apparatus 47 August 18, 2024, 4:04pm

> heinzl:
>
> Inside the sys-vpn terminal right?

Yes.

> heinzl:
>
> Then I get the same answer.

Try this command:

```
sudo sg qvpn -c "curl https://1.1.1.1"
```

or

```
sudo sg qvpn -c "curl https://9.9.9.9"
```

heinzl 48 August 18, 2024, 4:10pm

At the first command, after one or two seconds I just got an empty input line without giving me informations, after the second command before the empty input line it says “not found”.

apparatus 49 August 18, 2024, 4:13pm

Then network is working, it’s just an issue with DNS resolution in sys-vpn.
What’s in your /etc/resolve.conf in sys-vpn?

heinzl 50 August 18, 2024, 4:20pm

In the resolve.conf is

nameserver 10.139.1.1
nameserver 10.139.1.2

apparatus 51 August 18, 2024, 4:52pm

I don’t know why DNS resolution is not working for you.
You can use firewall counters/logs or tcpdump in sys-net and sys-whonix to check the how the DNS packets are handled.

heinzl 52 August 18, 2024, 5:40pm

Hm, ok, thanks for your help, but that getting to hard for me respectively I don’t want to spend more and more time on that. I am happy, that it worked with normal vpn and if I need Tor, I use it only.
Thanks again.

rand0023 53 August 29, 2024, 8:25pm

Hey guys, I have a similar issue.
My setup looks like this:
Tor → VPN1 → VPN2 → Clearnet

I am well aware of dangers of using VPN this way, I’ve been reading the documentation for two weeks non stop. This is a specific need, and VPN2 is disposable, while VPN1 is also disposable, just lives a little bit longer. They are just for few VMs, while the majority of my work happens using just sys-whonix.

Now my issue.
I have Qubes v4.2 and I have set it up using iptables and CLI scripts with the adjustments etaz provided, the later ones in the comment too.
In my sys-whonix I have disabled the transparent gateway and I am strictly using stream

isolation.

For VPN1, in ovpn file I have set socks-proxy to my sys-whonix and its working fine, while VPN2 does not have it.

For both of them resolv.conf has the virtual DNS. 10.139.x.x
When I am echoing the DNS servers qubes-vpn-handler sets the vpn_dns to - it shows something like 192.168.x.x . My understanding is that it is pulling VPN nameservers.

The conenctivity is fine, just the DNS is broken similar to previous comments. I have to manually change resolv.conf in VPN2 to some public DNS server (lets say 8.8.8.8), and do the same on the VM that connects to it to get things working. (the machine is win10 standalone VM).

I understand that thanks to sys-whonix I am still protected, but every time I do that I have a very uncomfortable feeling.

I need help to properly set this up so I can be sure it works as expected.
My understanding was that I could chain these qubes without issues, but it does not seem to be the case.
Here’s my files. Can anyone help me please get this right and understand the solution? I suspect something needs to be adjusted in firewall rules, but I am not very well versed here to make changes.

qubes-firewall-user-script:

```
#!/bin/bash
#    Block forwarding of connections through upstream network device
#    (in case the vpn tunnel breaks):
# Prevent the qube to forward traffic outside of the VPN
nft insert rule qubes custom-forward oifname eth0 counter drop
nft insert rule ip6 qubes custom-forward oifname eth0 counter drop
nft insert rule qubes custom-forward iifname eth0 counter drop
nft insert rule ip6 qubes custom-forward iifname eth0 counter drop



#   Block output hook
#nft 'add chain qubes output { type filter hook output priority 0; policy dro
#    Accept traffic to VPN
nft 'add chain qubes output { type filter hook output priority 0; policy acce
#iptables -P OUTPUT ACCEPT
#iptables -F OUTPUT

#    Add the `qvpn` group to system, if it doesn't already exist
if ! grep -q "^qvpn:" /etc/group ; then
     groupadd -rf qvpn
     sync
fi
sleep 2s

#    Block non-VPN traffic to clearnet
nft insert rule ip qubes output oifname eth0 counter drop
```

qubes-vpn-handler.sh

```
#!/bin/bash
set -e
export PATH="$PATH:/usr/sbin:/sbin"

case "$1" in

up)
# To override DHCP DNS, assign DNS addresses to 'vpn_dns' env variable before
# Format is 'X.X.X.X  Y.Y.Y.Y [...]'
if [[ -z "$vpn_dns" ]] ; then
    # Parses DHCP foreign_option_* vars to automatically set DNS address tran
    for optionname in ${!foreign_option_*} ; do
        option="${!optionname}"
        unset fops; fops=($option)
        if [ ${fops[1]} == "DNS" ] ; then vpn_dns="$vpn_dns ${fops[2]}" ; fi
    done
fi


nft flush chain ip qubes dnat-dns
#nft add chain qubes nat { type nat hook prerouting priority dstnat\; }
#iptables -t nat -F PR-QBS
if [[ -n "$vpn_dns" ]] ; then
    # Set DNS address translation in firewall:
    for addr in $vpn_dns; do
        nft add rule qubes dnat-dns iifname == "vif*" tcp dport 53 dnat "$add
```

---

apparatus 54 August 30, 2024, 9:18am

> rand0023:
>
> For both of them resolv.conf has the virtual DNS. 10.139.x.x
> When I am echoing the DNS servers qubes-vpn-handler sets the vpn_dns to - it shows something like 192.168.x.x . My understanding is that it is pulling VPN nameservers.
>
> The conenctivity is fine, just the DNS is broken similar to previous comments. I have to manually change resolv.conf in VPN2 to some public DNS server (lets say 8.8.8.8), and do the same on the VM that connects to it to get things working. (the machine is win10 standalone VM).

Is 192.168.x.x DNS server accessible?
Maybe it's just not working, then you can override it in the qubes-vpn-handler.sh:

> rand0023:
>
> ```
> # To override DHCP DNS, assign DNS addresses to 'vpn_dns' env variable be
> # Format is 'X.X.X.X  Y.Y.Y.Y [...]'
> ```

rand0023 55 August 30, 2024, 12:30pm

Yes, 192.168.x.x is accessible, and if I set the nameserver manually in resolv.conf - it works.
The same goes for public dns.

I have modified the script by adding echo “$vpn_dns”, echo “$addr”; echo “$option” in respective places to see what values they get.
When I pass dhcp-options in ovpn, qubes-vpn-handler correctly recognizes both the nameservers I set and the ones VPN server sets.
lets say I have in my ovpn file:

```
dhcp-options 8.8.8.8
dhcp-options 8.8.4.4
```

The output looks like this (these are the custom echo lines I have added to qubes-vpn-handler to see values):

```
Link is UP;
Foreign option: dhcp-option DNS 8.8.8.8
Setting Nameserver:  8.8.8.8
Foreign option: dhcp-option DNS 8.8.4.4
Setting Nameserver:  8.8.8.8 8.8.4.4
Foreign option: dhcp-option DNS 192.168.x.x
Setting Nameserver:  8.8.8.8 8.8.4.4 192.168.x.x
Address: 8.8.8.8
Address: 8.8.4.4
Address: 192.168.x.x
2024-08-30 08:04:43 Initialization Sequence Complete
```

/etc/resolv.conf still has the virtual nameservers that don’t work:

```
nameserver 10.139.1.1
nameserver 10.139.1.2
```

Here’s the nft ruleset after the initialization is complete:

```
$ 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
```

Overriding vpn_dns does not work as well, I have tried to pass values or modify the script directly. It is possible that I have messed up and set wrong firewall rules when compiling the info in this topic, but I cannot spot the problem.

---

apparatus 56 August 30, 2024, 12:39pm

Are you checking if DNS work in the VPN qube itself?
Check it in the qubes connected to the VPN qube.
If you don't plan to run anything in VPN qube itself that will require DNS resolution then you don't need to update /etc/resolve.conf. The DNS requests coming from the qubes connected to the VPN qube will be redirected to the correct DNS servers using firewall rules in `dnat-dns` chain.
If you want for openvpn to update /etc/resolve.conf then you need to install `resolvconf` and use `update-resolv-conf` up/down script:

NetworkManager is not changing /etc/resolv.conf after openvpn dns push

domain-name-system, openvpn, resolv.conf, networkmanager

answered by **Wenbing Li** on **04:18AM - 28 Mar 14 UTC**

---

rand0023 57 August 30, 2024, 1:04pm

Thank you very much!
Yes, I have been checking the DNS in the VPN Qube, and indeed it works in the connected AppQubes without manually changing the nameservers!

Thanks for clarifying!