

OpenWRT Policy Based Routing (PBR)

Latest iteration can be found at:

[https://raw.githubusercontent.com/egc112/OpenWRT-egc-add-on/main/notes/OpenWRT%20Policy%20Based%20Routing%20\(PBR\).pdf](https://raw.githubusercontent.com/egc112/OpenWRT-egc-add-on/main/notes/OpenWRT%20Policy%20Based%20Routing%20(PBR).pdf)

Version 12

Index

Introduction.....	1
Manual method with netifd.....	2
Default route.....	2
Manual Method removing Default route via the VPN.....	2
WireGuard disable default route via VPN:.....	2
OpenVPN disable default route via VPN:.....	3
Creating Routing tables via the VPN.....	3
Creating Routing tables via the WAN.....	4
Creating ip rules.....	5
IPv4.....	5
IPv6.....	6
NFTSET (ipset).....	8
1. Create nftset in firewall.....	8
2. Create nftset in DNSMasq.....	9
3. Create Firewall rules to mark traffic.....	9
4. Create routing table and routing rules.....	12

Introduction

When using a VPN usually all traffic is routed via the VPN. But sometimes you want to make an exempt for some traffic to use the WAN instead of the VPN.

This is done with the help of Policy Based Routing (PBR).

Policy Based Routing (PBR) works by creating routing tables and ip rules that specify which routing table to use when certain criteria are met.

Criteria for routing decision can be source and destination ip address, port, interface, domain name, fwmark etc. see: [ip rule man page](#)

A good starting point for using PBR in OpenWRT is the [OpenWRT PBR Wiki](#).

The [OpenWRT PBR Wiki](#) covers three main items which can be used for PBR.

This document will discuss the manual method using [netifd](#).

The [PBR app](#) which is the swiss army knife of PBR including a GUI is covered in the excellent [PBR app install and user guide](#). For simple needs e.g. a specific lan client, interface or port, the manual method using netifd will do but if you have more elaborate needs installing the full [PBR app](#) is the way to go. For MWAN3 see the [MWAN3 wiki](#).

Testbed

Dynalink DL-WRX36 main/snapshot build from 25-jul-2025

WireGuard VPN client to mullvad setup according to the [WireGuard Client Setup guide](#)

This guide uses LuCi to set things up but the resulting **config files** are also listed. The screenshots are made with OpenWRT2020 theme but that is not much different from the default theme.

Manual method with [netifd](#)

Default route

First we cover the default routing.

A typical VPN setup using Wireguard or OpenVPN will route all traffic via the VPN.

If most of the traffic indeed uses the VPN and if you want to keep it that way then proceed to [Creating Routing tables via the WAN](#).

But if you want most of the traffic to use the WAN then disable the default route via the VPN and make a routing table and ip rules to manually route the desired traffic via the VPN.

Manual Method removing Default route via the VPN

WireGuard disable default route via VPN:

There are three ways to disable the WireGuard VPN default route

1. **Disable (untick) Route Allowed IPs**

LuCi > Interfaces > WireGuard Interface > Peers > Edit Peer

Route Allowed IPs

☐

Optional. Create routes for Allowed IPs for this peer.

/etc/config/network:

```
config wireguard_wg_mullv_us
    option description 'mullvad-us-bos-wg-002.conf'
    option public_key 'LXXXXXX'
    option persistent_keepalive '25'
    option endpoint_host '43.225.189.162'
    option endpoint_port '51820'
    list allowed_ips '0.0.0.0/0'
    list allowed_ips '::0/0'
    list allowed_ips '8000::/1'
    list allowed_ips '::0/1'
    option route_allowed_ips '0'
```

Note Disabled is the default so you can also remove the option `route_allowed_ips`

2. **Uncheck Default Gateway**

LuCi > Interfaces > WireGuard interface > Advanced Settings:

Use default gateway

☐

If unchecked, no default route is configured

/etc/config/network:

```
config interface 'wg_mullv_us'
    option proto 'wireguard'
    option private_key 'YGaBrXXXXXX'
    list addresses '10.68.89.7/32'
    list addresses 'fc00:bbbb:bbbb:bb01::5:5906/128'
    list dns '10.64.0.1'
    option defaultroute '0'
```

This method can be useful if you have multiple routes in the Allowed IPs which you want to use and only want to stop default routing but keep the other routes enabled.

3. Use **OptionTable**

This method will remove the default route via the VPN **and** make an alternate routing table with default route via the VPN.

Important is that you keep the default route via the interface intact as the OptionTable method will move the default route from the main routing table to an alternate routing table.

This only works if you have one VPN with a default route, if you have multiple VPN's then see above, use

[Disable \(untick\) Route Allowed IPs](#) or [Uncheck Default Gateway](#)

To remove the default route via the VPN and make a new alternate routing table with table number 100:

LuCi > interfaces > WireGuard interface > Advanced options:

Override IPv4 routing table

100

Override IPv6 routing table

100

/etc/config/network:

```
config interface 'wg_mullv_us'
    option proto 'wireguard'
    option private_key 'YGaBrMXXXXXX'
    list addresses '10.68.89.7/32'
    list addresses 'fc00:bbbb:bbbb:bb01::5:5906/128'
    list dns '10.64.0.1'
    option ip4table '100'
    option ip6table '100'
```

For various reasons it is not feasible to use the option table method to make an alternate routing table via the **WAN**, if you want this then use the other methods mentioned.

OpenVPN disable default route via VPN:

Add in the OpenVPN config:

For IPv4 only:

pull-filter ignore "redirect-gateway"

For IPv6:

pull-filter ignore "redirect-gateway ipv6"

pull-filter ignore "route-ipv6 0000::/2"

pull-filter ignore "route-ipv6 4000::/2"

pull-filter ignore "route-ipv6 8000::/2"

pull-filter ignore "route-ipv6 C000::/2"

pull-filter ignore "route-ipv6 2000::/3"

Creating Routing tables via the VPN

If you use the [OptionTable method](#) then the routing table is automatically created, for the other methods you must create the routing tables as described below.

Create alternate VPN routing table with default route via the VPN:

LuCi > Network > Routing > Static IPv4 Routes > Add:

You specify

Interface: *<your WireGuard interface>*

Target: *0.0.0.0/0*

On Advanced Settings the table number:

Table: *100* (this is an arbitrary number)

Table: 100

General Settings Advanced Settings

Interface

wg_mullv_us:  

Specifies the logical interface name of the parent (or master) interface

Route type

unicast

Specifies the route type to be created

Target

0.0.0.0/0

Network address

Gateway

192.168.0.1

Specifies the network gateway. If omitted, the gateway from the parent interface is used. If set to 0.0.0.0 no gateway will be specified.

Advanced Settings:

Table

100

Routing table into which to insert this rule.

You do the same for Static IPv6 routes but you use as Target: `::0/0`

`/etc/config/network:`

```
config route
    option interface 'wg_mullv_us'
    option target '0.0.0.0/0'
    option table '100'
```

```
config route6
    option interface 'wg_mullv_us'
    option target ':::/0'
    option table '100'
```

For OpenVPN you have to add the OpenVPN interface in the Network section and then use that interface for making your routing table.

As device you use the device which is set in your OpenVPN config e.g.: `dev tun0` if only `dev tun` is set then OpenVPN uses the first available tunnel number so it will be `tun0`

Creating Routing tables via the WAN

This works exactly as making routing tables via the VPN the only difference is that you use as interface "wan/wan6" and set the gateway. The gateway is the nexthop which can be get from the command line with

For IPv4: `ifstatus wan | grep nexthop`

For IPv6: `ifstatus wan6 | grep nexthop`

Interface: wan/wan6

Gateway: <next hop>

`/etc/config/network:`

```
config route
    option interface 'wan'
    option target '0.0.0.0/0'
    option gateway '192.168.0.1'
    option table '100'
```

```
config route6
    option interface 'wan6'
    option target ':::/0'
    option gateway 'fe80::bef5:81ff:fc4e:82a2'
```

option table '100'

You can check routing with (from command line):

```
ip route show
```

```
ip route show table 100
```

```
ip -6 route show
```

```
ip -6 route show table 100
```

For the record I also added the use of *Option Table* to remove Default route of the VPN and making an alternate routing table see: [Using Option Table to remove VPN default route](#)

Note if you want to use a string as table_id instead of a number you have to add the number and string to `/etc/iproute2/rt_tables`

Creating ip rules

Now that we have an alternate routing table we are going to create rules which are used to create policies with which you specify which clients, ports, interfaces etc are going to use these alternate routing tables.

IPv4

Example for setting one LAN client (192.168.1.8) to use the Alternate routing table 100

LuCi > Network > routing > IPv4 Rules: Add

General Settings:

- **Priority:** *2000* (Optional)
- **Rule Type:** *unicast* (default)
- **Incoming interface:** *unspecified* (default)
- **Source:** *192.168.1.8/32* (the IP address of your LAN client in CIDR notation, you can also set a whole subnet)
- **IP protocol:** *unspecified* (default)
- **Outgoing interface:** *unspecified* (default)
- **Destination:** *0.0.0.0/0* (default)

Routing

General Settings Advanced Settings

Priority	<input type="text" value="2000"/> <small>Execution order of this IP rule: lower numbers go first</small>
Rule type	<input type="text" value="unicast"/> <small>Specifies the rule target routing action</small>
Incoming interface	<input type="text" value="unspecified"/> <small>Match traffic from this interface</small>
Source	<input type="text" value="192.168.1.8/32"/> <small>Match traffic from this source subnet (CIDR notation)</small>
IP Protocol	<input type="text" value="unspecified"/> <small>Match traffic IP protocol type</small>
Outgoing interface	<input type="text" value="unspecified"/> <small>Match traffic destined to this interface</small>
Destination	<input type="text" value="0.0.0.0/0"/> <small>Match traffic destined to this subnet (CIDR notation)</small>

Advanced Settings:

Table: *100* (Dropdown box: choose *custom* and set the table number of the alternate routing table)

Routing

General Settings Advanced Settings

Table

100

Routing table to use for traffic matching this rule.
A numeric table index, or symbol alias declared in `/etc/ipr`
main (254) and default (253) are also valid
Matched traffic re-targets to an interface using this table.

For a **whole subnet** use as **Source:** `192.168.1.0/24`

For an **interface** e.g. your lan interface use: **Outgoing interface:** `lan`

For a **source port**, useful if you want to route the port of a WireGuard server via the wan in case you also have a Wireguard client with default route via the VPN, on Advanced Settings > **Source Port:** `51820`

`/etc/config/network:`

```
config rule
    # for ip source:
    option src '192.168.1.8/32' or '192.168.1.0/24'
    # destination e.g. from all to dest
    option dest '25.52.71.40/32'
    # for interface
    option in 'lan'
    # for proto
    option ipproto 'icmp'
    # for source port
    option sport '51820'
    # for destination port
    option dport '116'
    #table number to use for lookup
    option lookup '100'
    option priority '2000'
```

For using local routes in your new routing table, which usually is a good idea, add `suppress_prefixlength` with lower priority so that the local routes of the main table will be used:

`/etc/config/network:`

```
config rule 'policy_localroute'
    option lookup 'main'
    option suppress_prefixlength '1'          # See note
    option priority '1000'                    # lower priority then other rules so that it is hit first
```

IPv6

For IPv6 you do the same on **LuCi > Network > routing > IPv6 Rules**

Using source addresses is much more difficult as your lan clients will often use temporary IPv6 addresses so use ULA or LL addresses

`/etc/config/network:`

```
config rule6
    # for ip source: this is difficult as IPv6 uses temporary addresses, consider
    using the ULA or LL addresses
    # for interface
    #option in 'lan'
    # for proto
    option ipproto 'icmp'
    # for source port
    option sport '51820'
```

```
# for destination port
option dport '116'
#table number to use for lookup
option lookup '100'
option priority '2000'
```

For Local IPv6 routes:

```
config rule6 'policy_localrt6'
    option lookup 'main'
    option suppress_prefixlength '1'          # See note
    option priority '1000'                    # lower priority then other rules so that it is hit first
```

Note about suppress_prefixlength:

For suppress_prefixlength a value of '1' is chosen and not '0' because OpenVPN and also sometimes for WireGuard, the default route is overridden by using e.g. 128.0.0.0/1 and 0.0.0.0/1.

A suppress_prefixlength of '1' will suppress both /1 and /0 (default) routes.

Some VPN providers even use /4 routes for IPv6 default routing, in that case you should use a value of '4'

NFTSET (ipset)

<https://forum.openwrt.org/t/manual-setup-to-bypass-wireguard-vpn-for-udp-traffic-with-specific-source-port/242798/2?u=egc>
<https://forum.openwrt.org/t/using-ipset-by-domain-from-luci-in-23-05/176870>

Using nftset's (before fw4 it was called ipset but that name is still used but under the hood it is an nft set) is a four step procedure.

Prerequisite: you need to have installed DNSMasq-full !

1. Create nftset in firewall

Create the IPSET in the firewall this will make an nftset. Create an nftset for IPv4 with the 4 suffix and if applicable for IPv6 with the 6 suffix.

For further firewall rules (step 3) make sure you use for Packet field Match: *dest_net*, as this is a destination.

Firewall rules will then be made with *daddr* instead of *saddr*. This is because for firewall traffic rules you normally enter *source* or *destination* but if you use an nftset you only set the nftset to use, so in this field you specify the nftset is used as *source* or *destination*.

Network > Firewall > IP set:

Firewall - IP sets

Name	<input type="text" value="domain-to-wan4"/>
Comment	<input type="text" value="Comment"/>
Family	<input type="text" value="IPv4"/>
Packet Field Match	<div><input type="text" value="dest_net: Destination (sub)net"/><div>-</div></div> <div>-- Please choose -- ▾</div> <div>Packet fields to match upon. Syntax: <i>direction_datatype</i>. e.g.: <i>src_port</i>, <i>dest_r</i> Directions: <i>src</i>, <i>dst</i>. Datatypes: <i>ip</i>, <i>port</i>, <i>mac</i>, <i>r</i> Direction prefixes are optional. *Note: datatype <i>set</i> is unsupported in fw4.</div>
IPs/Networks/MACs	<div><input type="text"/><div>+</div></div> <div>macaddr[ip[/cidr]]</div>
Max Entries	<div><input type="text"/></div> <div>up to 65536 entries.</div>
Include File	<div>Select file...</div> <div>Path to file of CIDRs, subnets, host IPs, etc.</div>
Timeout	<div><input type="text" value="0"/></div> <div>Unit: seconds. Default 0 means the entry is added Max: 2147483 seconds.</div>
Counters	<div><input type="checkbox"/></div> <div>Enables packet and byte count tracking for the se</div>

Make two rules one for ipv4 and one for ipv6 with a 6 suffix:

domain-to-wan4	ipv4	dest_net	none	none	<input checked="" type="checkbox"/>
domain-to-wan6	ipv6	dest_net	none	none	<input checked="" type="checkbox"/>


```
etc/config/firewall:
config ipset
    option name 'domain-to-wan4'
    option family 'ipv4'
    list match 'dest_net'
```

```
config ipset
    option name 'domain-to-wan6'
    option family 'ipv6'
    list match 'dest_net'
```

2. Create nftset in DNSMasq

Create an nftset for DNSMasq, because you already have made an nftset in the firewall you can choose this as name, add both IPv4 and IPv6

Network > DNS > IP set:

Edit IP set

Name of the set	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">domain-to-wan4</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">domain-to-wan6</div> <div style="border: 1px solid #ccc; padding: 2px;">-- Please choose --</div>
FQDN	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">ipleak.net</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;"></div> <div style="border: 1px solid #ccc; padding: 2px;">+</div>
Netfilter table name	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">fw4</div> <div style="font-size: 0.8em;">Defaults to fw4.</div>
Table IP family	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 2px;">IPv4+6</div> <div style="font-size: 0.8em;">Defaults to IPv4+6. Can be hinted by adding 4 or 6 to the name. Adding an IPv6 to an IPv4 set and vice-versa silently fails.</div>

```
/etc/config/dhcp:
config ipset
    list domain 'ipleak.net'
    option table_family 'inet'
    list name 'domain-to-wan4'
    list name 'domain-to-wan6'
```

This should result in /tmp/etc/dnsmasqXXX:
nftset=/ipleak.net/inet#fw4#domain-to-wan4,6#inet#fw4#domain-to-wan6

3. Create Firewall rules to mark traffic

Create a rule in the firewall to use this set to mark traffic

A rule on the *mangle_output* chain is for marking traffic from the router itself e.g from DNSMasq.

A rule in the forward *mangle_prerouting* chain is for marking traffic from local lan clients.

For traffic from the router itself (mangle_output chain) we can use Luci (netifd):

Network > Firewall > Traffic Rules:

Firewall - Traffic Rules - mark-wan-output4

General Settings	Advanced Settings	Time Restrictions
Name	mark-wan-output4	
Protocol	Any	
Source zone	Device(output)	
Source address	-- add IP --	
Output zone	Any zone	
Destination address	-- add IP --	
Action	apply firewall mark	
Set mark	0x00000100/0x0000ff00	
Set the given mark value on established connec		

Arbitrary firewall mark *0x00000100* is chosen with accompanying mask: *0x0000ff00*

The above is for IPv4, for IPv6 repeat with IPv6 nftset source and IPv6 address family.

Both IPv4 and IPv6 rules have this in Advanced settings:

Firewall - Traffic Rules - mark-wan-forward4

General Settings	Advanced Settings	Time Restrictions
Match device	unspecified	
Restrict to address family	IPv4 only	
Use ipset	domain-to-wan4	
Source MAC address	-- add MAC --	
Match helper	any	
Match traffic using the specified connection tracking help		
Match mark		
Matches a specific firewall mark or a range of different mc		
Match DSCP	any	
Matches traffic carrying the specified DSCP marking.		
Limit matching	unlimited	
Limits traffic matching to the specified rate.		
Enable logging	<input type="checkbox"/>	
Log matched packets to syslog.		

etc/config/firewall:

```
config rule
    option dest '*'
    option name 'mark-wan-output4'
    option target 'MARK'
    option set_mark '0x00000100/0x0000ff00'
    option ipset 'domain-to-wan4'
```

```
option family 'ipv4'
list proto 'all'
```

```
config rule
option dest '*'
option name 'mark-wan-output6'
option target 'MARK'
option set_mark '0x00000100/0x0000ff00'
option ipset 'domain-to-wan6'
option family 'ipv6'
list proto 'all'
```

To mark traffic for routing we need to make a rule in the *prerouting* chain as the mark must be set before the routing. unfortunately I have not found a way to use uci/netifd for making rules in the *mangle_prerouting* chain so just do it the hard way with:

```
nft 'add rule inet fw4 mangle_prerouting ip daddr @domain-to-wan4 counter meta mark set meta mark &
0xffff01ff | 0x00000100 comment "!fw4: mark-wan-forward4"'
```

```
nft 'add rule inet fw4 mangle_prerouting ip6 daddr @domain-to-wan6 counter meta mark set meta mark &
0xffff01ff | 0x00000100 comment "!fw4: mark-wan-forward6"'
```

To make it persistent see:

https://openwrt.org/docs/guide-user/firewall/firewall_configuration#includes_2203_and_later_with_fw4
https://openwrt.org/docs/guide-user/firewall/netfilter_iptables/netfilter_openwrt

In this case I add the rules to:

```
/usr/share/nftables.d/chain-pre/mangle_prerouting/10-nftrouting.nft:
ip daddr @domain-to-wan4 counter meta mark set meta mark & 0xffff01ff | 0x00000100
comment "!fw4: mark-wan-forward4";
ip6 daddr @domain-to-wan6 counter meta mark set meta mark & 0xffff01ff | 0x00000100
comment "!fw4: mark-wan-forward6";
```

Make sure each rule ends with a semi colon

If the rules are used e.g. for REJECT instead of for marking traffic for routing then L(uci) can be used to make a rule in the FORWARD chain:

```
config rule
option dest '*'
option name 'mark-wan-forward4'
option target 'MARK'
option set_mark '0x00000100/0x0000ff00'
option ipset 'domain-to-wan4'
option src '*'
option family 'ipv4'
list proto 'all'
```

```
config rule
option dest '*'
option name 'mark-wan-forward6'
option target 'MARK'
option set_mark '0x00000100/0x0000ff00'
option ipset 'domain-to-wan6'
option src '*'
```

```
option family 'ipv6'  
list proto 'all'
```

4. Create routing table and routing rules

Make a routing table for a route to the wan with table 100 [described above](#)
Network > Routing

/etc/config/network (this is an example [see above for correct settings](#)):

```
config route  
    option interface 'wan'  
    option gateway '192.168.0.1'  
    option table '100'  
    option target '0.0.0.0/0'  
  
config route6  
    option interface 'wan6'  
    option target '::0/0'  
    option gateway 'fe80::1628:c0ff:fe6b:123a'  
    option table '100'
```

Make an ip rule to route traffic with mark 0x00000100/0x0000ff00 lookup table 100, I use priority 50
Network > Routing

Routing	
General Settings	Advanced Settings
Priority	<input type="text" value="50"/> Execution order of this IP rule: lower numbers go first
Rule type	<input type="text" value="unicast"/> Specifies the rule target routing action
Incoming interface	<input type="text" value="unspecified"/> Match traffic from this interface
Source	<input type="text" value="0.0.0.0/0"/> Match traffic from this source subnet (CIDR notation)
IP Protocol	<input type="text" value="unspecified"/> Match traffic IP protocol type
Outgoing interface	<input type="text" value="unspecified"/> Match traffic destined to this interface
Destination	<input type="text" value="0.0.0.0/0"/> Match traffic destined to this subnet (CIDR notation)

Firewall mark on the Advanced tab:

Routing

General Settings Advanced Settings

Table

100 ▼

Routing table to use for traffic matching this rule.
A numeric table index, or symbol alias declared in `/etc/iproute2/rt_tables`.
Special aliases local (255), main (254) and default (253) are available.
Matched traffic re-targets to an interface using this table.

Jump to rule

80000

Jumps to another rule specified by its priority value

Firewall mark

0x00000100/0x0000ff00

Specifies the fwmark and optionally its mask to match, e.g. C or 0x0/0x1 to match any even mark value

Repeat for IPv6

`/etc/config/network:`

`config rule`

`option priority '50'`

`option mark '0x00000100/0x0000ff00'`

`option lookup '100'`

`config rule6`

`option priority '50'`

`option lookup '100'`

`option mark '0x00000100/0x0000ff00'`