

# How to configure pfSense as multi wan (DUAL WAN) load balance failover router

Author: Vivek Gite Last updated: July 15, 2021 [32 comments](#)



How do I setup a multi-WAN load balancing and failover on pfSense router with two ADSL or cable or leased-line or FTTH (Fiber to the home) connections?

In this tutorial you will learn how to configure pfSense to load balance and fail over traffic from a LAN to multiple Internet connections (WANs) i.e. dual wan.

Tutorial details	
Difficulty level	<a href="#">Advanced</a>
Root privileges	<a href="#">Yes</a>
Requirements	pfSense firewall
Est. reading time	7 minutes

## Why and how to setup a dual wan router?

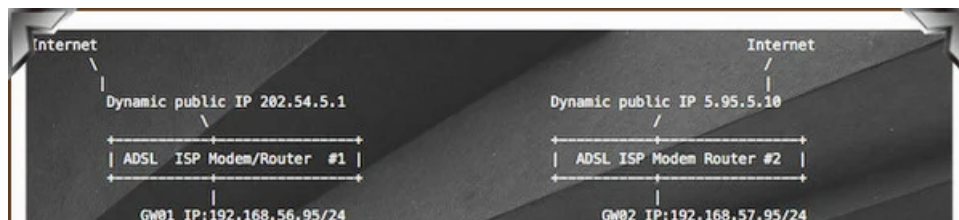
A dual wan setup allows you to increase your internet bandwidth. You can load balance traffic as per your needs. You can get internet connection redundancy and failover. If one connection goes down your traffic will be routed automatically to a backup connection.

## Requirements

Two internet connections from two different ISPs. You can mix-match ADSL/FTTH/4G LTE/Cable/T1/FIOS connection as per your needs.

1. pfSense router with three network ports (NICs).
2. Two ISP modems with network port (NIC)
3. Static or dynamic IPs from ISPs
4. Monitor IP # 1 for ISP # 1 – 8.8.8.8 (google dns IP)
5. Monitor IP # 2 for ISP # 2 – 208.69.38.205 (opendns IP)

## Our sample setup



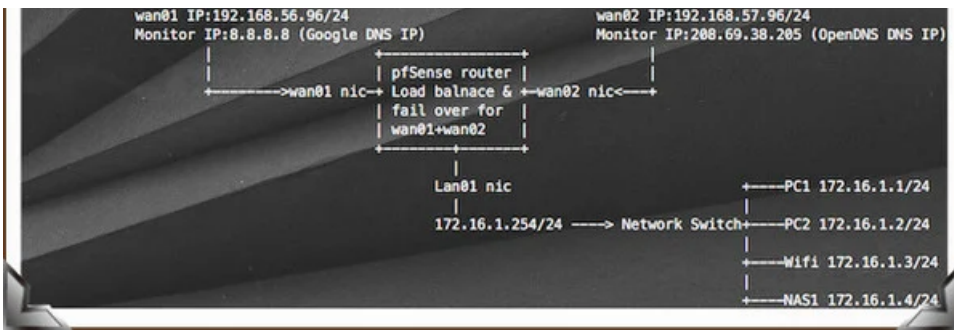


Fig.01: What you'll need to get started with this setup

1. I have two ISP modems+routers with dynamic IP address assigned.
2. You need to connect each modem with pfsense using an Ethernet connection.
3. You need to connect a network switch to pfsense using an Ethernet connection.
4. All systems/servers/printers/wifi on LAN uses 172.16.1.254/24 subnet with 172.16.1.254 as a default gateway.

## Configuration

Before starting, make sure all of the WAN-type interfaces are enabled with static IP WANs and with a gateway set as described above.

### Step 1: Configure pfsense LAN interface

Open pfSense web interface using <http://172.16.1.254/> > Interfaces > LAN and set it as follows as per (fig.01):

The screenshot shows the pfSense web interface for configuring the LAN interface. The 'General Configuration' section is visible, with the following settings:
 

- Enable:**  Enable interface
- Description:** LAN
- IPv4 Configuration Type:** Static IPv4
- IPv6 Configuration Type:** None
- MAC Address:** xxxxxxxxxxxxxx
- MTU:** (blank)
- MSS:** (blank)
- Speed and Duplex:** Default (no preference, typically autoselect)

 The 'Static IPv4 Configuration' section is also visible, with the following settings:
 

- IPv4 Address:** 172.16.1.254 / 24
- IPv4 Upstream gateway:** None

 Red arrows in the image point to the 'Enable interface' checkbox, the 'Static IPv4' dropdown, the '172.16.1.254' IP address field, and the 'None' dropdown for the upstream gateway. A green button labeled '+ Add a new gateway' is also visible next to the gateway dropdown.

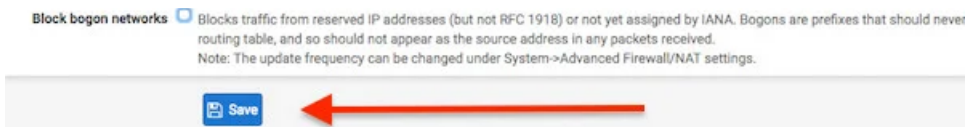


Fig.02: LAN interface settings

## Step 2: Configure pfsense wan01 interface (ADSL ISP #1)

Open pfSense web interface using <http://172.16.1.254/> > Interfaces > WAN 01 and set it as follows as per (fig.01):

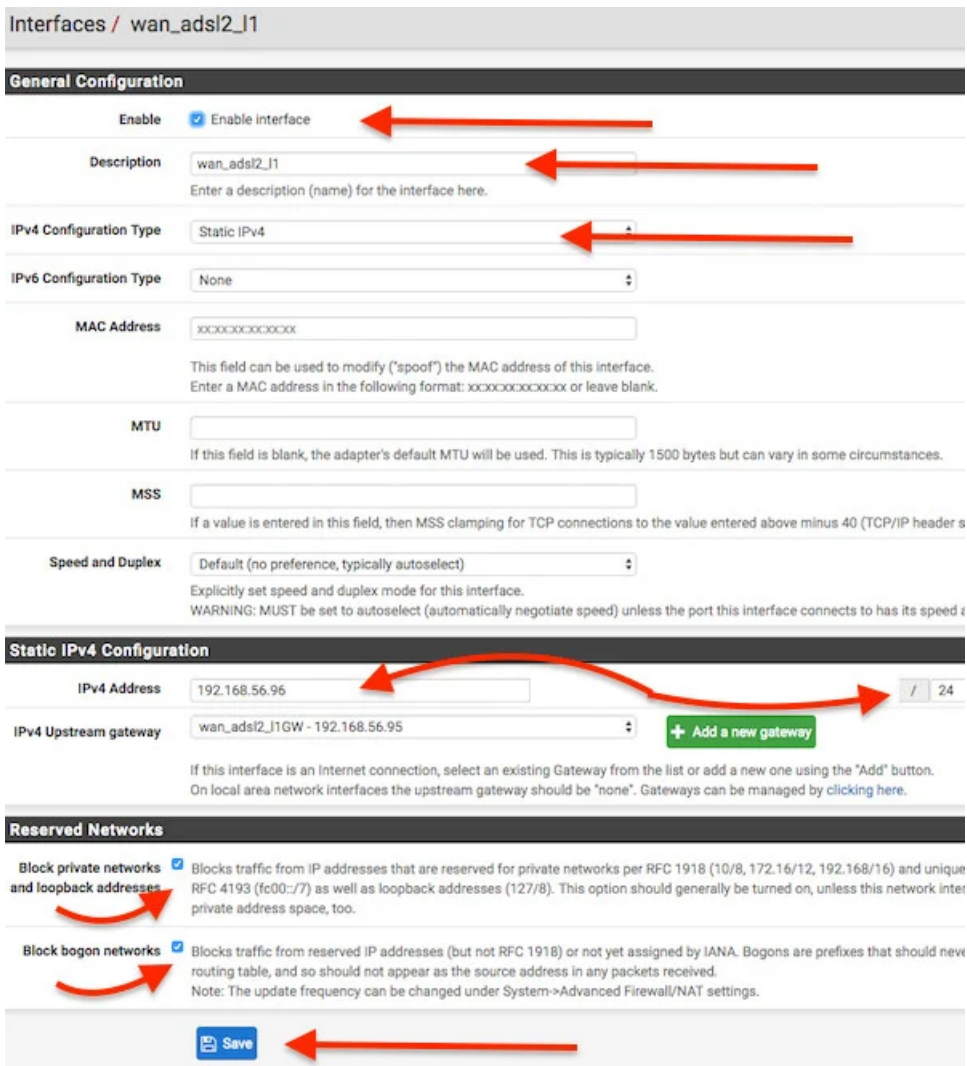


Fig.02: Wan 01 (ADSL ISP 1) interface settings

Now the first WAN interface configured with a Static IP from the Interfaces menu. If you want you can set type to DHCP depending on your ISP 1 modem settings. Next make sure the gateway IP responds to ping to confirm that WAN 1 is actually online and working before proceeding. You can do this from pfSense itself by visiting **Diagnostics > Ping**:

**Diagnostics / Ping**

**Ping**

Hostname: 192.168.56.96

IP Protocol: IPv4

Source address: Automatically selected (default)  
Select source address for the ping.

Maximum number of pings: 3  
Select the maximum number of pings.

**Ping**

**Results**

```

PING 192.168.56.96 (192.168.56.96): 56 data bytes
64 bytes from 192.168.56.96: icmp_seq=0 ttl=64 time=0.052 ms
64 bytes from 192.168.56.96: icmp_seq=1 ttl=64 time=0.369 ms
64 bytes from 192.168.56.96: icmp_seq=2 ttl=64 time=0.071 ms

--- 192.168.56.96 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.052/0.164/0.369/0.145 ms

```

Make sure the ISP #1 gateway responds to ping to confirm that each WAN 1 is actually online

### Step 3: Configure pfSense wan02 interface (ADSL ISP #2)

Open pfSense web interface using <http://172.16.1.254/> > Interfaces > WAN 02 and set it as follows as per (fig.01):

**Interfaces / wan\_adsl2\_l2**

**General Configuration**

Enable:  Enable interface

Description: wan\_adsl2\_l2  
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xxxxxxxxxx  
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxx or leave blank.

MTU:   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:   
If a value is entered in this field, then MSS clamps to the value entered above minus 40 (TCP/IP header s

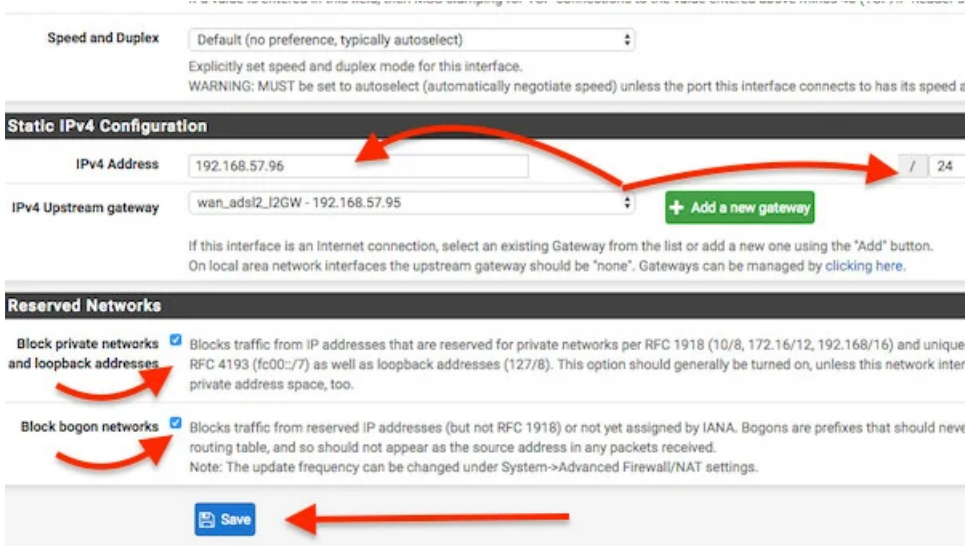
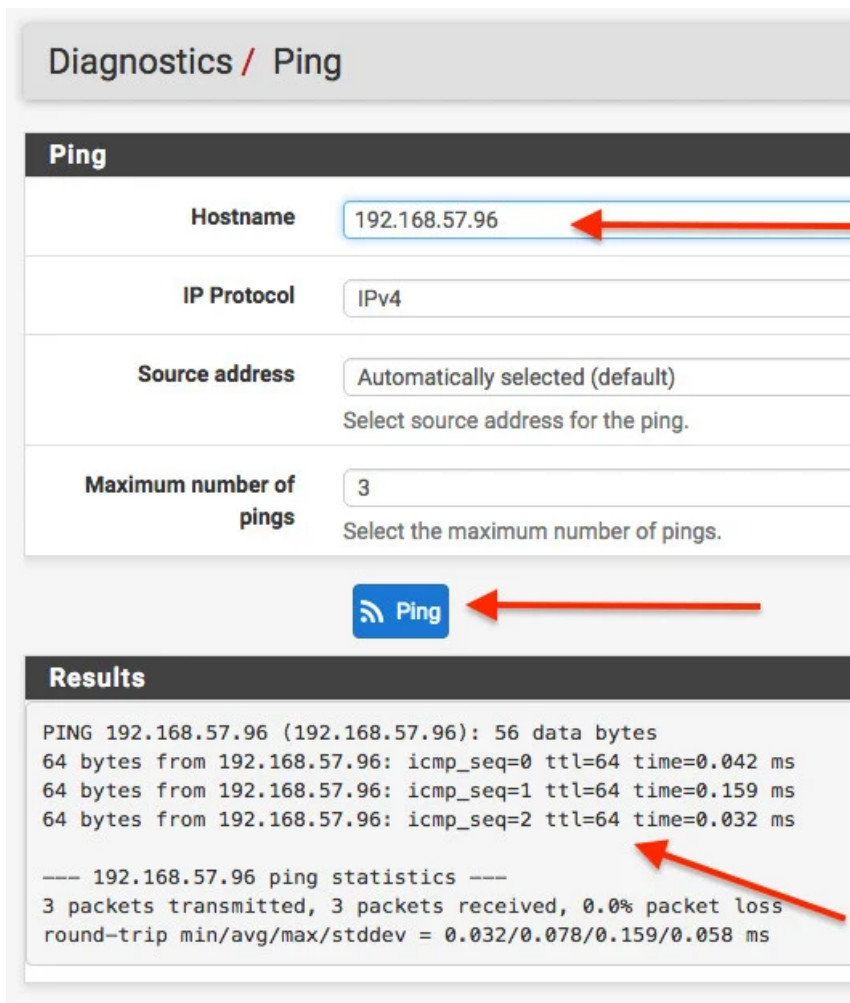


Fig.03: Wan 02 (ADSL ISP 2) interface settings

Now the second WAN interface configured with a Static IP from the Interfaces menu. If you want you can set type to DHCP depending on your ISP 2 modem settings. Next make sure the gateway IP responds to ping to confirm that WAN 2 is actually online and working before proceeding. You can do this from pfSense itself by visiting **Diagnostics > Ping**:



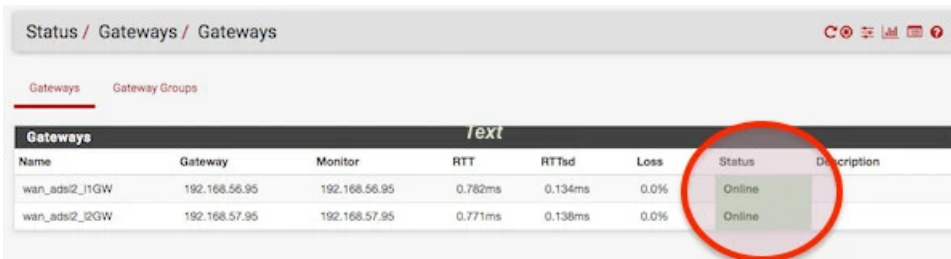
Make sure the ISP #2 gateway responds to ping to confirm that each WAN 2 is actually online



make sure the wan\_2 gateway responds to ping to confirm that each WAN 2 is actually online

## Step 4: Confirm both gateways are online

Once both gateways have been defined, visit **Status > Gateways**:



The screenshot shows the 'Status / Gateways / Gateways' page. A table lists two gateways: wan\_adsl2\_1GW and wan\_adsl2\_2GW. The 'Status' column for both is 'Online', which is highlighted in green. A red circle is drawn around the 'Status' column header and the 'Online' entries.

Name	Gateway	Monitor	RTT	RTTsd	Loss	Status	Description
wan_adsl2_1GW	192.168.56.95	192.168.56.95	0.782ms	0.134ms	0.0%	Online	
wan_adsl2_2GW	192.168.57.95	192.168.57.95	0.771ms	0.138ms	0.0%	Online	

Fig.04: Wan gateways status must be green

If they're green, the connection to the gateway is OK and you need to configure monitor IP.

## Step 5: Configure monitor IP for each gateway

Visit **System > Routing > Select Gateways tab** and you will see a screen as follows with private IP set as monitor IP for each gateway:



The screenshot shows the 'System / Routing / Gateways' page. A table lists two gateways: wan\_adsl2\_1GW (default) and wan\_adsl2\_2GW. The 'Monitor IP' column shows private IP addresses (192.168.56.95 and 192.168.57.95). Red arrows point from blue text boxes to the 'Monitor IP' column and the 'Actions' column (specifically the edit icon). A green '+ Add' button is visible at the bottom right.

Name	Interface	Gateway	Monitor IP	Description	Actions
wan_adsl2_1GW (default)	WAN_ADSL2_L1	192.168.56.95	192.168.56.95		[edit] [copy] [refresh] [delete]
wan_adsl2_2GW	WAN_ADSL2_L2	192.168.57.95	192.168.57.95		[edit] [copy] [refresh] [delete]

Fig.05: Ensure a gateway entry exists for each WAN interface

Click on **edit gateway** icon (button) for wan\_adsl2\_1GW (default) and set monitor IP to 8.8.8.8:

System / Routing / Gateways / Edit ↻ 🔍 📊

### Edit Gateway

**Disabled**  Disable this gateway  
Set this option to disable this gateway without removing it from the list.

**Interface**   
Choose which interface this gateway applies to.

**Address Family**   
Choose the Internet Protocol this gateway uses.

**Name**   
Gateway name

**Gateway**   
Gateway IP address

**Default Gateway**  This will select the above gateway as the default gateway.

**Gateway Monitoring**  Disable Gateway Monitoring  
This will consider this gateway as always being up.

**Monitor IP**   
Enter an alternative address here to be used to monitor the link. This is used for the qu  
RRD graphs as well as the load balancer entries. Use this if the gateway does not resp  
ICMP echo requests (pings).

**Force state**  Mark Gateway as Down  
This will force this gateway to be considered down.

**Description**   
A description may be entered here for reference (not parsed).

Fig.06: Set monitor IP for WAN 1 (ADSL ISP # 1)

Next, click on **edit gateway** icon (button) for WAN\_ADSL2\_L2 (ADSL ISP # 2) and set monitor IP to 208.69.38.205:

System / Routing / Gateways / Edit ↻ 🔍

### Edit Gateway

**Disabled**  Disable this gateway  
Set this option to disable this gateway without removing it from the list.

**Interface**   
Choose which interface this gateway applies to.

**Address Family**   
Choose the Internet Protocol this gateway uses.

**Name**   
Gateway name

**Gateway**   
Gateway IP address

**Default Gateway**  This will select the above gateway as the default gateway.

**Gateway Monitoring**  Disable Gateway Monitoring  
This will consider this gateway as always being up.

**Monitor IP**   
Enter an alternative address here to be used to monitor the link. This is used in RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).

**Force state**  Mark Gateway as Down  
This will force this gateway to be considered down.

**Description**   
A description may be entered here for reference (not parsed).

Fig.07: Set monitor IP for WAN 2 (ADSL ISP # 2)

The gateway configuration has been changed. The changes must be applied for them to take effect. So click on the **Apply Changes** button.

System / Routing / Gateways

The gateway configuration has been changed.  
The changes must be applied for them to take effect.

Gateways Static Routes Gateway Groups

Gateways						
Name	Interface	Gateway	Monitor IP	Description	Actions	
<input checked="" type="checkbox"/> wan_adsl2_l1GW (default)	WAN_ADSL2_L1	192.168.56.95	8.8.8.8	ADSL ISP # 1 Gateway	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> wan_adsl2_l2GW	WAN_ADSL2_L2	192.168.57.95	208.69.38.205	ADSL ISP # 2 Gateway	<input type="checkbox"/>	<input type="checkbox"/>

## Step 6: Configuring dual WAN link load balancer

Finally, you are ready to configure the pfSense as a Load Balancer by visiting **System > Routing > Select the Gateway Groups > Click the "Add" button:**



System / Routing / Gateway Groups / Edit

### Edit Gateway Group Entry

**Group Name**  1

**Gateway Priority**

<input type="text" value="wan_adsl2_I1GW"/>	<input type="text" value="Tier 1"/> <span>2</span>	<input type="text" value="Interface Address"/>	<input type="text" value="ADSL ISP # 1 Gateway"/>
<input type="text" value="wan_adsl2_I2GW"/>	<input type="text" value="Tier 1"/> <span>3</span>	<input type="text" value="Interface Address"/>	<input type="text" value="ADSL ISP # 2 Gateway"/>

Gateway	Tier	Virtual IP	Description

**Link Priority** The priority selected here defines in what order failover and balancing of links will be done. Multiple link priority will balance connections until all links in the priority will be exhausted. If all links in a priority level the next available link(s) in the next priority level will be used.

**Virtual IP** The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic OpenVPN endpoint.

**Trigger Level**  4  
When to trigger exclusion of a member

**Description**  5  
A description may be entered here for administrative reference (not parsed).

6

Fig.08: Dual wan load balancer config

Where,

- Set **Group Name** to "WanLoadBalancer".
- Set **Gateway Priority** for both gateways to "Tier 1". Please note that when two gateways are on the same tier (e.g. Tier 1), they will load balance. This means that on a per-connection basis, connections are routed over each WAN in a round-robin manner. If any gateway on the same tier goes down, it is removed from use and the other gateways on the tier continue to operate normally.
- Set **Trigger Level** to "Memberdown".
- Set **Description** to "My Dual ADSL Wan Link Load Balancer"
- Finally click the "Save" > "Apply Changes" button.

## Step 7: Configuring link fail over

Next, configure the pfSense as a failover for wan connections by visiting

System > Routing > Select the **Gateway Groups** > Click the "Add" button:

System / Routing / Gateway Groups / Edit

**Edit Gateway Group Entry**

Group Name: ADSLLinkFailover2 **1**

Gateway Priority

Gateway	Tier	Virtual IP	Description
wan_adsl2_l1GW	Tier 1 <b>2</b>	Interface Address	ADSL ISP # 1 Gateway
wan_adsl2_l2GW	Tier 2 <b>3</b>	Interface Address	ADSL ISP # 2 Gateway

Link Priority: The priority selected here defines in what order failover and balancing of links will be done. Multiple link priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted, the next available link(s) in the next priority level will be used.

Virtual IP: The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic OpenVPN endpoint.

Trigger Level: Member down **4**  
When to trigger exclusion of a member

Description: Link failover for ADSL 1 **5**  
A description may be entered here for administrative reference (not parsed).

Save **1**

Fig.09: Link failover for ADSL link 1 (wan1/isp1)

When two gateways are on different tiers, the lower tier gateway(s) are preferred. If a lower tier gateway goes down, it is removed from use and the next highest tier gateway is used. This is how failover works on pfSense. So to set link failover for ADSL 1:

- Set **Group Name** to "ADSLLinkFailover2"
- Set **Gateway Priority** wan\_adsl2\_l1GW (ISP 1) to "Tier 1"
- Set **Gateway Priority** wan\_adsl2\_l2GW (ISP 2) to "Tier 2"
- Set **Trigger Level** to "Member down"
- Set **Description** to "Link failover for ADSL 1"

Set link failover for ADSL 2 as follows and swap Gateway Priority:

System / Routing / Gateway Groups / Edit

**Edit Gateway Group Entry**

Group Name: ADSLLinkFailover1 **1**

Gateway Priority

Gateway	Tier	Virtual IP	Description
wan_adsl2_l1GW	Tier 2 <b>2</b>	Interface Address	ADSL ISP # 1 Gateway
wan_adsl2_l2GW	Tier 1 <b>3</b>	Interface Address	ADSL ISP # 2 Gateway

Link Priority: The priority selected here defines in what order failover and balancing of links will be done. Multiple link priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted, the next available link(s) in the next priority level will be used.

Virtual IP: The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic OpenVPN endpoint.

Save **1**

OpenVPN endpoint.

**Trigger Level** Member down 4  
When to trigger exclusion of a member

**Description** Link failover for ADSL 2 5  
A description may be entered here for administrative reference (not parsed).

**Save** 6

Fig.10: Link failover for ADSL link 2 (wan2/isp2)

Finally click the **"Save" > "Apply Changes"** button to finish the LB and failover gateway configuration.

## Step 7: Configuring the firewall rules for load balancer

You need to pass traffic to these LBs using the Gateway setting on firewall rules. Click on **Firewall > Rules > Lan > Add** and set it as follows:

**Edit Firewall Rule**

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST port unreachable for UDP) is returned to the sender, whereas with block the packet silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** LAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** any  
Choose which IP protocol this rule should match.

**Source**

**Source**  Invert match LAN net Source Address

**Destination**

**Destination**  Invert match any Destination Address

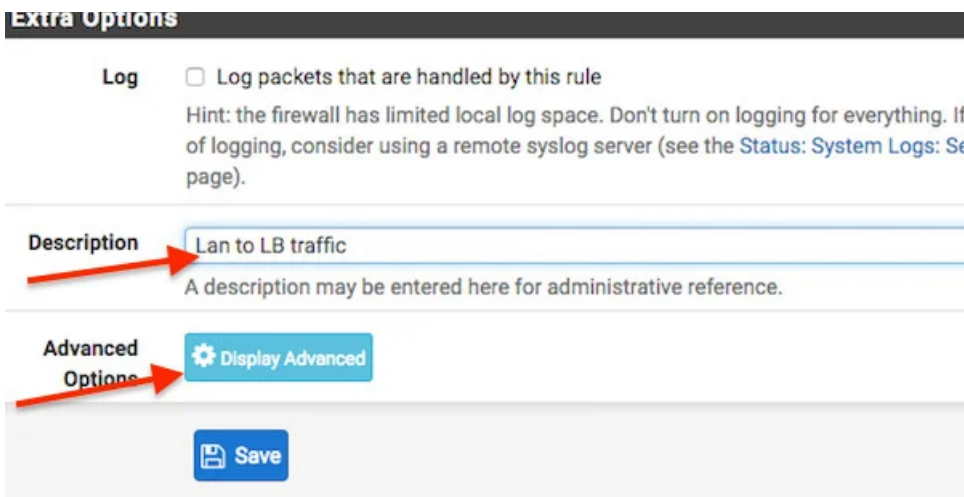
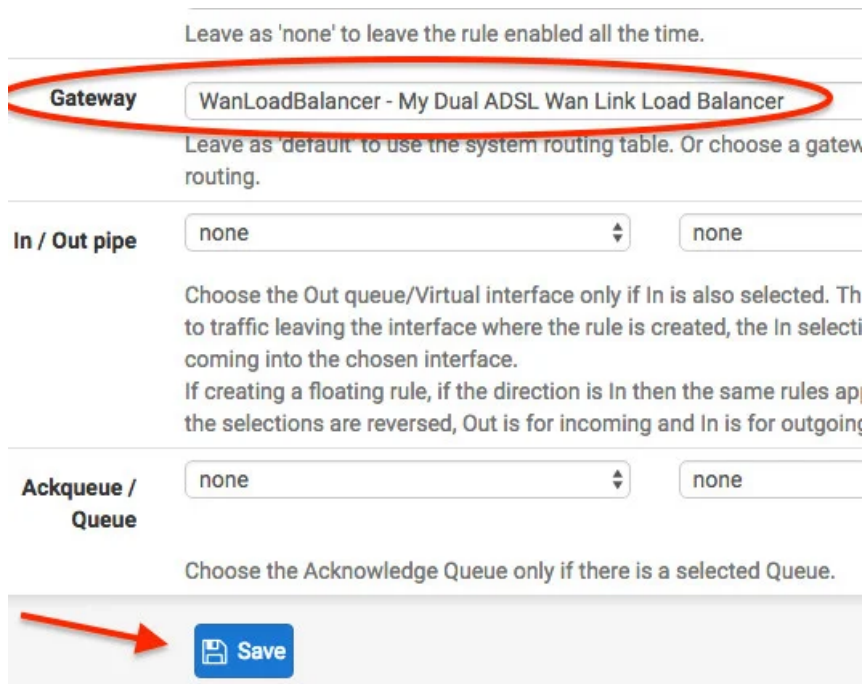


Fig.11: LB firewall rule

Click on the “**Display advanced**” button > scroll down > find Gateway option and set it to WanLoadBalancer:



Set gateway to WanLoadBalancer

Click the “Save” > “Apply Changes” button to save firewall rules.

## Step 8: Configuring the firewall rules for failover

You need to pass traffic to these failover gateways using the Gateway setting on firewall rules. Click on **Firewall** > **Rules** > **Lan** > **Add** and set it as follows:

**Edit Firewall Rule**

**Action**

Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RS port unreachable for UDP) is returned to the sender, whereas with block the packet is discarded silently. In either case, the original packet is discarded.

**Disabled**

Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface**

LAN

Choose the interface from which packets must come to match this rule.

**Address Family**

IPv4

Select the Internet Protocol version this rule applies to.

**Protocol**

any

Choose which IP protocol this rule should match.

**Source**

**Source**

Invert match

LAN net

Source Address

**Destination**

**Destination**

Invert match.

any

Destination Address

**Extra Options**

**Log**

Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If you need a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**

Adsl link failover 1]

A description may be entered here for administrative reference.

**Advanced Options**

Display Advanced

**Gateway**

ADSLLinkFailover1 - Link failover for ADSL 2

Leave as 'default' to use the system routing table. Or choose a gateway to utilize routing.

**In / Out pipe**

none

none

Choose the Out queue/Virtual interface only if In is also selected. The Out selection applies to traffic leaving the interface where the rule is created, the In selection is applied to traffic coming into the chosen interface.

If creating a floating rule, if the direction is In then the same rules apply, if the direction is Out then the same rules apply, if the direction is In then the same rules apply, if the direction is Out then the same rules apply.

Fig.12: Failover firewall rule for ISP 1 /ADSL 1 link


Click on the "Display advanced" button > scroll down > find Gateway option and set it to ADSLLinkFailover1:



the selections are reversed, Out is for incoming and in is for outgoing.

Ackqueue / Queue

Choose the Acknowledge Queue only if there is a selected Queue.



Set gateway to ADSLLinkFailover1

Click the "Save" > "Apply Changes" button to save firewall rules. Repeat the firewall rule for ADSLLinkFailover2.

## Step 9: Client configuration

Make sure you assign all the IP addresses in the following range to your client computers:

- Network: 172.16.1.254/24
- IP ranges: 172.16.1.1 to 172.16.1.253
- Default gateway: 172.16.1.254
- DNS server: 172.16.1.254 (or 8.8.8.8/8.8.4.4)

Test it as follows from client system (I'm using OpenBSD):

```
$ ifconfig vio0
```

```
$ netstat -nr -f inet
```

```
$ ping -c 2 google.com
```

```
$ host cyberciti.biz 172.16.1.254
```

Sample outputs:

```
bash-4.3$ ifconfig vio0
vio0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    lladdr 08:00:27:6a:0c:9d
    priority: 0
    groups: egress
    media: Ethernet autoselect
    status: active
    inet 172.16.1.201 netmask 0xfffff00 broadcast 172.16.1.255
bash-4.3$ netstat -nr -f inet
Routing tables

Internet:
Destination      Gateway          Flags    Refs      Use     Mtu  Prio  Iface
default          172.16.1.254    UGS      4          8       -    8    vio0
127/8            127.0.0.1      UGRS     0          0 32768  8    lo0
127.0.0.1       127.0.0.1      UH1      0          0 32768  1    lo0
172.16.1/24     172.16.1.201   UC        2          0       -    4    vio0
172.16.1.1     0a:00:27:00:02 UHLC     1          3       -    4    vio0
172.16.1.201   08:00:27:6a:0c:9d UHL1     0          20      -    1    vio0
172.16.1.254   08:00:27:2b:b1:3f UHLC     1          9       -    4    vio0
172.16.1.255   172.16.1.201   UHb      0          0       -    1    vio0
224/4           127.0.0.1      URS      0          0 32768  8    lo0
bash-4.3$ ping -c 2 google.com
PING google.com (216.58.197.78): 56 data bytes
64 bytes from 216.58.197.78: icmp_seq=0 ttl=53 time=16.252 ms
64 bytes from 216.58.197.78: icmp_seq=1 ttl=53 time=16.636 ms
--- google.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 16.252/16.444/16.636/0.192 ms
bash-4.3$ host cyberciti.biz 172.16.1.254
Using domain server:
Name: 172.16.1.254
Address: 172.16.1.254#53
Aliases:

cyberciti.biz has address 74.86.144.194
cyberciti.biz mail is handled by 1 exch1.google.com
```

```
cyberciti.biz mail is handled by 1 aspmx1.google.com.  
cyberciti.biz mail is handled by 10 aspmx2.googlemail.com.  
cyberciti.biz mail is handled by 10 aspmx3.googlemail.com.  
cyberciti.biz mail is handled by 5 alt1.aspmx1.google.com.  
cyberciti.biz mail is handled by 5 alt2.aspmx1.google.com.  
bash-4.3$
```

Fig.13: Testing your pfSense LB/Failover router

You can run a speed test using [fast.com](http://fast.com) or [speedtest.net](http://speedtest.net). You will notice and use both internet connection when using Torrents and downloading a large file from load balancing. You can [use the speedtest-cli as follows to verify that bandwidth is doubled](#) from a client computer:

```
$ python speedtest-cli
```

If one internet connections goes down, you will be still connected via

failover.

## What next?

You will get the wan (internet) connection redundancy and load balancing but not the router redundancy. Your internet connection will go down, if your pfSense router failed due to hardware problems. This draw back can be addressed using router redundancy setup.