



Gateways Static Routes Gateway Groups

**Gateways**

Name	Interface	Gateway	Monitor IP	Description	Actions
vpn_gw (default)	WAN	172.17.20.22	172.17.20.22		
WAN_DHCP	WAN	172.17.20.254	172.17.20.254	Interface WAN_DHCP Gateway	

[+ Add](#)

Gateways Static Routes Gateway Groups

**Static Routes**

Network	Gateway	Interface	Description	Actions
192.168.1.0/32	vpn_gw - 172.17.20.22	WAN	client-vpn	

[+ Add](#)

## Ping

<b>Hostname</b>	<input type="text" value="192.168.42.22"/>
<b>IP Protocol</b>	IPv4
<b>Source address</b>	Automatically selected (default)
	Select source address for the ping.
<b>Maximum number of pings</b>	3
	Select the maximum number of pings.



## Results

```

PING 192.168.42.22 (192.168.42.22): 56 data bytes
64 bytes from 192.168.42.22: icmp_seq=0 ttl=128 time=0.689 ms
64 bytes from 192.168.42.22: icmp_seq=1 ttl=128 time=0.498 ms
64 bytes from 192.168.42.22: icmp_seq=2 ttl=128 time=0.548 ms

--- 192.168.42.22 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.498/0.578/0.689/0.081 ms

```

## IPv4 Routes

Destination	Gateway	Flags	Use	Mtu	Netif	Expire
default	172.17.20.22	UGS	626	1500	vmx0	
127.0.0.1	link#3	UH	3662	16384	lo0	
172.17.20.0/24	link#1	U	26931	1500	vmx0	
172.17.20.98	link#1	UHS	0	16384	lo0	
192.168.1.0/32	172.17.20.22	UGS	0	1500	vmx0	
192.168.42.0/24	link#2	U	1044	1500	vmx1	
192.168.42.254	link#2	UHS	0	16384	lo0	
208.67.220.220	00:50:56:b3:9f:8b	UHS	18	1500	vmx0	
208.67.222.222	00:50:56:b3:9f:8b	UHS	18	1500	vmx0	

## IPv6 Routes

## Firewall Advanced

<b>IP Do-Not-Fragment compatibility</b>	<input type="checkbox"/> Clear invalid DF bits instead of dropping the packets
	This allows for communications with hosts that generate fragmented packets with the don't fragment (DF) bit set. Linux NFS is known to do this. This will cause the filter to not drop such packets but instead clear the don't fragment bit.
<b>IP Random id generation</b>	<input type="checkbox"/> Insert a stronger ID into IP header of packets passing through the filter.
	Replaces the IP identification field of packets with random values to compensate for operating systems that use predictable values. This option only applies to packets that are not fragmented after the optional packet reassembly.
<b>Firewall Optimization Options</b>	Normal
	The default optimization algorithm
<b>Disable Firewall</b>	<input checked="" type="checkbox"/> Disable all packet filtering.
	Note: This converts pfSense into a routing only platform! Note: This will also turn off NAT! To only disable NAT, and not firewall rules, visit the <a href="#">Outbound NAT</a> page.
<b>Disable Firewall Scrub</b>	<input checked="" type="checkbox"/> Disables the PF scrubbing option which can sometimes interfere with NFS traffic.
<b>Firewall Adaptive Timeouts</b>	<input type="text" value="Adaptive start"/> <input type="text" value="Adaptive end"/>
	<p>When the number of state entries exceeds this value, adaptive scaling begins. All timeout values are scaled linearly with factor (adaptive.end - number of states) / (adaptive.end - adaptive.start). Defaults to 60% of the Firewall Maximum States value</p> <p>When reaching this number of state entries, all timeout values become zero, effectively purging all state entries immediately. This value is used to define the scale factor, it should not actually be reached (set a lower state limit, see below). Defaults to 120% of the Firewall Maximum States value</p>



Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
-----------	----------	----------------	--------------	---------------	-------------	--------	-----------	-------------	---------

↑ Add
↓ Add
🗑 Delete
💾 Save
+ Separator



Outbound NAT Mode

Mode

- Automatic outbound NAT rule generation. (IPsec passthrough included)
- Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation. (No Outbound NAT rules)

💾 Save

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
-----------	--------	-------------	-------------	------------------	-------------	----------	-------------	-------------	---------

↑ Add
↓ Add
🗑 Delete
💾 Save



NPt Mappings

Interface	External Prefix	Internal prefix	Description	Actions
-----------	-----------------	-----------------	-------------	---------

↑ Add
↓ Add
🗑 Delete
💾 Save

Ping

**Hostname**

**IP Protocol**

**Source address** 
  
Select source address for the ping.

**Maximum number of pings** 
  
Select the maximum number of pings.

📡 Ping

Results

```

PING 172.17.20.22 (172.17.20.22): 56 data bytes
64 bytes from 172.17.20.22: icmp_seq=0 ttl=64 time=0.179 ms
64 bytes from 172.17.20.22: icmp_seq=1 ttl=64 time=0.208 ms
64 bytes from 172.17.20.22: icmp_seq=2 ttl=64 time=0.164 ms

--- 172.17.20.22 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.164/0.184/0.208/0.018 ms
    
```