











Firewall Rules


The last step of your WireGuard set up involved creating 2 firewall rules. One for your WAN firewall, and one for your Tunnel.

If you haven't done so already, assign your WireGuard VPN as an interface. To do so, navigate to Interfaces ---> Assignments:


INTERFACES: ASSIGNMENTS		
Interface	Identifier 	Device
[HomeWGVPN]	opt2	 wg0 (WireGuard - HomeWGVPN) 
[LAN]	lan	 igb0 (a0:36:9f:2f:85:b0) 
[WAN]	wan	 igb1 (a0:36:9f:2f:85:b1) 
[homeLAB1]	opt1	 igb3 (a0:36:9f:2f:85:b3) 
		

Select your Interface in the sidebar menu:


Basic configuration

 Enable


☒ Enable Interface

 Lock


☒ Prevent interface removal

 Identifier

opt2


 Device

wg0


 Description

HomeWGVPN


Generic configuration

 Block private networks


☐


 Block bogon networks

☐


 IPv4 Configuration Type


None




 IPv6 Configuration Type


None




 MAC address

 Promiscuous mode

☐

 MTU

 MSS

- Enable the interface
- Lock to prevent removal

- No other configs need to be done, save changes and apply settings.

WAN Rule

Navigate to Firewall ---> Rules ---> WAN and create a new rule:

FIREWALL: RULES: WAN

Edit Firewall rule

- Action**: Pass
- Disabled**: ☐ Disable this rule
- Quick**: ☒ Apply the action immediately on match.
- Interface**: WAN
- Direction**: in
- TCP/IP Version**: IPv4+IPv6
- Protocol**: UDP
- Source / Invert**: ☐ Use this option to invert the sense of the match.
- Source**: any
- Source**: Advanced
- Destination / Invert**: ☐ Use this option to invert the sense of the match.
- Destination**: WAN address
- Destination port range**:

from:	to:
(other)	(other)
51823	51823
- Log**: ☒ Log packets that are handled by this rule

OPNsense (c) 2014-2024 Deciso B.V.

Select the following settings for the rule:

- Action = Pass
- Quick - checked
- Interface = WAN
- Direction = In
- TCP/IP Version = IPv4 + IPv6
- Protocol = UDP
- Source = ANY
- Destination = WAN Address
- Destination Port Range = Enter your Port Number you designated earlier
 - Default WireGuard port is 51820
- Save and apply rules

WireGuard Interface Rule

Navigate to your Firewall ---> Rules ---> Select your WireGuard Interface then click create:

FIREWALL: RULES: HOMEWGVN

Edit Firewall rule

Action	Pass
Disabled	<input type="checkbox"/> Disable this rule
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.
Interface	HomeWGVN
Direction	in
TCP/IP Version	IPv4+IPv6
Protocol	any
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Source	HomeWGVN net
Source	Advanced
Destination / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Destination	any
Destination port range	from: any to: any
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule
Category	

IPNsense (c) 2014-2024 Deciso B.V.

This rule will allow your client to access any device on the local network. Configure the following settings:

- Action = Pass
- Quick = Checked
- Interface = WireGuard Interface
- Direction = In
- TCP/IP Version = IPv4 + IPv6
- Protocol = any
- Source = Select your WireGuard Interface Net as source
- Destination = Any
- Save and apply rules.

Your configuration should now be all set. Check out the next page to view results!

Revision #3

Created 1 April 2024 19:47:56 by Austin

Updated 1 April 2024 20:24:49 by Austin