OPNsense as a 44Net router/firewall



Contents

Abstract	1
Assumptions	2
Requirements	2
Obtain a POP account	2
Set up the VPN	3
Eirewall rules	6
Test the VPN	6

Abstract

The aim of this document is to walk the reader through the steps necessary to connect their OPNsense router/firewall to the 44Net Wireguard VPN service.

Assumptions

A functioning OPNsense firewall with all the current patches and updates with at least 2 network ports is already installed. Familiarity with the OPNsense user interface.

Requirements

44Net Wireguard VPN credentials 44Net subnet allocation (optional)

Obtain a POP account

Create a POP access account at https://pop.44net.cloud. Then request a tunnel. Ensure to click the refresh button at the end of the "Preshared Key (optional)" box. A Preshared Key will ensure even greater security (Wireguard is very secure in itself).

	NODE Apollo	70115	VPN1 Fremont CA
	Eastern-Atlanta Vultr Atlanta	Europe Vultr - Frankfurt	Western-California Fremont_Huricane Electric
	Interface_1 44.33.1.0/24, 2a0a:bb06:1::/48	O user 44.33.3.0/26, 2a0a:bb06:2:1::/64	Interface_1 44.31.197.0/24
Name (Optional)		
Name (NI20 Give your	Optional) Documentation walkthrough tunnel a name to help you identify it.		
Name (NI2O Give your Public K	Optional) Documentation walkthrough tunnel a name to help you identify it. Key (Optional)		
Name (NI2O Bive your Public K	Optional) Documentation walkthrough tunnel a name to help you identify it. Key (Optional) not provide a public key, we will generate you a p	rivate key for you.	
Name (NI2O Give your Public K f you do r Preshar vKX+	Optional) Documentation walkthrough tunnel a name to help you identify it. Key (Optional) not provide a public key, we will generate you a p ed Key (Optional) ·NWOLbljVbnzT7iqrG3cnoIDZqw3	rivate key for you. Copkpw21hQ9A=	
Name (NI2O Give your Public K f you do r Preshar vKX+	Optional) Documentation walkthrough tunnel a name to help you identify it. (ey (Optional) not provide a public key, we will generate you a p ed Key (Optional) NWOLbljVbnzT7iqrG3cnoIDZqw3 ed key offers an added layer of security.	rivate key for you. Copkpw21hQ9A=	
Name (f NI2O Give your Public K If you do r Preshar VKX+ A preshar	Optional) Documentation walkthrough tunnel a name to help you identify it. Gey (Optional) not provide a public key, we will generate you a p red Key (Optional) NWOLbljVbnzT7iqrG3cnoIDZqw3 ed key offers an added layer of security. c Routing (Optional)	rivate key for you. Copkpw21hQ9A=	
Name ((NI2O Give your Public K If you do r Preshar VKX+ A preshar Dynamic Dynamic	Optional) Documentation walkthrough tunnel a name to help you identify it. Gey (Optional) not provide a public key, we will generate you a p ed Key (Optional) NWOLbljVbnzT7iqrG3cnoIDZqw3 ed key offers an added layer of security. c Routing (Optional) one	rivate key for you. Copkpw21hQ9A=	

Tunnel details

Your tunnel has been successfully created! Please find the details below.

Your Configuration

Private key—Keep this in a secure place, as it cannot be shown to you again. UL2w9J94MmentAp0NNIXLdgR6o/LktozHyImq5 XTQ2U=

Public key

AcazL4JfynIjXBQ7p+ssQwVZEXhhBxTmxQZ9B1 yXRWA=

Allocations

44.31.197.62/32

Server Configuration

Public key Eq2CoxEu9ekfB+DkxCAJyjjRJYzR38xNAdvR1r zk9Fc=

Preshared key
vKX+NWOLbIjVbnzT7iqrG3cnolDZqw3Copkpw2
1hQ9A=

Endpoint 107.161.208.53:12346

Addresses 44.31.197.1

Configuration

Some example configurations to help get you started!

```
QRCode
```

wg-quick

```
[Interface]
PrivateKey = UL2w9J94MmentAp0NNIXLdgR6o/LktozHyImq5XTQ2U=
Address = 44.31.197.62/32
DNS = 1.1.1.1, 1.0.0.1
```

```
[Peer]
PublicKey = Eq2CoxEu9ekfB+DkxCAJyjjRJYzR38xNAdvR1rzk9Fc=
PresharedKey = vKX+NW0LbIjVbnzT7iqrG3cnolDZqw3Copkpw21hQ9A=
Endpoint = 107.161.208.53:12346
PersistentKeepalive = 10
AllowedIPs = 0.0.0.0/0, ::/0
```

Screenshot this webpage. It contains your keys. Ensure to copy the "wg-quick" information to a text file. In a separate file record your Public and Private keys from under the "Your Configuration" heading. This information will NEVER be shown again. Keep these files for later use.

Set up the VPN

Using the left side menu system navigate to VPN > Wireguard > Instances. Click the + sign on the right side of the screen to add a new VPN Instance. Populate all the fields on this form with the information you saved from your POP account files. Ensure to populate the IPv6 information as well as the traditional IPv4

Edit instance			×
 advanced mode 			full help 🛈
😢 Enabled		2	
i) Name		44Net-POP	
6 Instance			
🔋 Public key	٠	XoEQeE9TSGEahCCPqQABisrSjzzO7koZw4g+EVNYQ	
😢 Private key		8H8ey27QlQq68/H5NOyfiCzDMbxlE2fWo6t1mo4nfnU=	
🚯 Listen port		44444	
6 MTU		1384	
() DNS servers			
		8 Clear All 🖓 Copy 🖪 Paste 🖹 Text	
1 Tunnel address		44.33.1.32/32 × 2a0a:bb06:1::d/128 ×	
		🛚 Clear All 🖓 Copy 🖪 Paste 🖹 Text	
(i) Depend on (CARP)		None 🔻	
() Peers		44Net-POP -	
		Clear All	
1 Disable routes			
i) Gateway			
			Cancel Save

Be sure to populate the MTU field with a value of 1384. This will give you the best packet transfer over the VPN.

Click "Save" and then "enable" the instance

□ 🗹 44Net-POP wg1	Enabled	Name	Device
		44Net-POP	wgl

Move on to the "Peers" tab and click the + button over on the right.

Populate the fields with the data you saved earlier then click "Save"

Edit peer			×
4		fu	il help Ο
🚺 Enabled			
i) Name	44Net-POP		
🔋 Public key	CCK2lhIIo1BpAzqfQVUjPhVjFyslZ/R9Vh0AU1LJ218=		
1) Pre-shared key	WY8OUQRiErfenglOHzwon8oXGj5EvSFj1J9wt0Zfdpo=		
1 Allowed IPs	44.0.0.0/9 × 44.128.0.0/10 ×		
	😢 Clear All 🦨 Copy 📭 Paste 🖹 Text		
i) Endpoint address	45.32.220.92		
🚯 Endpoint port	12345		
Instances	44Net-POP 👻		
	Clear All		
i) Keepalive interval	10		
		Cancel	Save

Note that in the example above the "Allowed IP's" differ from your settings file. In this instance the VPN is only allowed to carry traffic going to and from the 44Net. If you need full Internet access (e.g. for your Echolink node) then set this field to 0.0.0/0 for IPv4 and ::/0 for IPv6.

Select the Instance you created just a few moments ago.

The "Keepalive Interval" setting is also important here. If you are behind a cable company router or any ISP that uses CGNAT (most cellphone and many Cable co's) your incoming VPN session will be interrupted after a very short time. Setting the "Keepalive" does exactly what it suggests; it keeps the VPN session alive. In the example above it is set for 10 seconds. You may experiment with this setting. The longer interval you set the Keepalive for the more secure your system will be (see the Wireguard documentation for an explanation of how traffic passes for this VPN method).

Finally, click the "Enable WireGuard" box and click "Apply".

1 Enable WireGuard	Z
Apply	

Firewall rules

We need firewall rules so as to allow our traffic to flow out to the 44Net and prevent bad traffic coming in from the 44Net (its an Internet network so safe sex rules apply!).

If you are simply connecting to the 44Net to access its services then your firewall rules will be simple: "deny" incoming and "allow" outgoing.

From the left side menu select Firewall > Rules > Wireguard (group) and then click the + button on the right to enter a new rule

FIREWALL: RULES: WII	REGUARD (GROUP)							Select category		 Inspect
The firewall rule configuration has been changed. You must apply the changes in order for them to take effect.									Apply changes		
-	Protocol	Source	Port	Destination	Port	Gateway	Schedule		Description 🛛		ڬ 🗲 🗊 🗹 🗆
<u>۵</u>									Automatically generated rules		O 16
■ × → † 0	IPv4+6*										
■ ► ← ¥ 8	IPv4+6 *										
 pass pass (disabled) 	× ×	block block (disabled)		🙁 reject 😣 reject (disab	led)		 log log (disabled) 		→ in ← out	 first match last match 	
🖹 🗎 Active/Inactive Schedule (click to view/edit)											
III Alias (click to view/edit)											
WireGuard (Group) rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.											

In the above example we have created a "deny" rule for incoming traffic and an "allow" rule for outgoing traffic. The deny rule is set to "block" incoming traffic rather than reject it. Again, this is a security feature. By "rejecting" traffic we confirm that there is in fact a server/service available to the incoming hacker. "Blocking" the traffic means that we quietly drop the data we don't want without responding to the sender. They will never know if there is in fact a service to connect to or not.

Finally "Apply" the changes.

Test the VPN

A simple test would be to ping a 44net address from your connected workstation. Try 44.1.1.17 (portal.ampr.org). To check that you are in fact going out over the VPN, perform a traceroute or MTR to any 44Net IP address (44.1.1.17 again?). Note that your first few hops should be 44Net addresses.