NORD VPN on opnSense

Setting up NordVPN on an opnsense router is poorly documented (several years old) and assumes all LAN traffic will be pushed through Nord.

This document will set up an opnSense firewall using the OpenVPN configuration for NordVPN. When done, all network traffic from the LAN will go through the NordVPN instance. Upon completion, you should have enough information to be able to add additional subnets (say, wireless, or part of it).

How do you know if it works? If you do not know your current public IP, visit https://www.whatsmyip.org/ and record it. The final step in these instructions suggest you visit this same site, and success is indicated when the IP Address returned is the IP address of the NordVPN service.

Note: In our case, we have a second VPN instance which should supercede the NordVPN for certain subnets. After you have completed these instructions, you can see how to do this in opnSense + NordVPN + otherVPN

Overview

Note: This document has been specifically written for the new OpenVPN setup which can be used in 2025, and will be the only one available in 2026.

Note: This document assumes you have a working opnSense firewall/router. There are other documents on how to do that. We also assume you have a valid NordVPN account.

1. Set Up NordVPN
    1. Configure NordVPN as an OpenVPN instance
        1. Test
    2. Set up a NordVPN interface
    3. Create an Outbound NAT entry to correctly NAT LAN traffic through the NordVPN
    4. Create a firewall rule to force all LAN traffic to use NordVPN
        1. Test

Set up NordVPN

While the Nord site has some instructions, they are really difficult to follow and have a lot of questions. Instead, we'll download a copy of the OpenVPN configuration file Nord provides, and get the username and password. With this information, we can create an OpenVPN Client instance in opnSense.

Get NordVPN information

1. Log into your NordVPN account at https://nordaccount.com/
    1. Go to **Advanced Settings** (you may need to scroll down) and select **Set up NordVPN**

Manually

2. Get credentials
    1. Select Credentials tab
    2. you may have to validate via e-mail
    3. copy your username and password to a secure file on your computer
3. Get openVPN configuration file
    1. Go to the **Server Recommendations** tab
        1. If you do not want to use the recommended server, select one from the list below
        2. If you want one of the servers not in your location, Select the OpenVPN Config Files tab
    2. Click **Get Setup Configuration** button (big blue button, as this is being written)
    3. Select OpenVPN (default)
    4. Select UDP or TCP (I prefer UDP for speed, choose TCP for stability)
    5. Save that file someplace convenient

Set up OpenVPN connection

We will be copying information from the ovpn file you downloaded from Nord. An ovpn file is kind of confusing to some people, so keep the following in mind:

A **block** means copying the data between two XML looking tags. So, for example, the *ca block* would be all of the lines between <ca> and </ca> in the ovpn file. The *tls-auth* block is everything between <tls-auth> and </tls-auth>. You do **not** include the <blockname> or the </blockname>, only the things between them

A **value** means to copy the value of a line. For example, the line *auth SHA512* has a name of *auth* and a value of *SHA512*, so you would only copy the latter (*SHA512*)

1. Open both documents you got from Nord (credentials, and open vpn configuration file)
2. Log into your opnSense router
3. Copy Nord Certificate of Authority
    1. Go to **System** | **Trust** | **Authorities**
    2. Add new (orange plus sign)
    3. Method: **Import an existing Certificate Authority**
    4. Description: **NordCA** (or anything memorable)
    5. Locate the <ca> block in the ovpn file and copy the contents (everything between <ca> and </ca>
    6. Paste that into the **Certificate Data** box
    7. Click **Save** (do not fill out anything else, leave them blank)
4. Copy the TLS Auth Key
    1. Go to **VPN** | **OpenVPN** | **Instances**
    2. Click **Static Keys** tab
    3. Click plus sign to add a new key
    4. Give it a good **Description** (I used 'NordVPN - ' and the URL to the endpoint server)
    5. Set **Mode** to **auth**
    6. open the ovpn file
        1. Locate block beginning with <tls-auth> and ending with </tls-auth>
        2. Copy everything *between* those lines (do not include the <tls-auth> stuff, but do include everything else)
    7. Paste contents of the <tls-auth> block from the ovpn file into **Static Key**

8. Click **Save** button

5. Set up the Instance
    1. Click the **Instance** Tab
    2. Add a new one by clicking the plus sign
    3. Click the **Advanced Mode** selector (upper left)
        1. Role: Client
        2. Description: NordVPN (or whatever you want)
        3. Protocol: same as **proto** in ovpn file
        4. Port Number: Find four digit number in ovpn file after the **remote**. Something like 1194
        5. Type: Same as **dev** in ovpn file
        6. Remote: IP address in **remote** line of ovpn (do not include the port)
            1. You can also use the DNS name, for example, I chose us8120.nordvpn.com, so I can use that
        7. Certificate Authority: Select the Certificate of Authority you imported (I called it NordCA)
        8. TLS static key: choose the static key you created in the previous block (dropdown)
        9. Auth: Use value of **auth** from ovpn file
        10. Username and Password: Use the username and password you downloaded from Nord (second file)
    4. Click Save button

At this point, you should have a VPN connection set up. To verify, go to **VPN** | **OpenVPN** | **Connection Status**. You should see an entry for NordVPN, and it should say **Connected**. Note that the first time you make this connection, it may take up to a minute to actually say **Connected**. Click the **Connection Status** link until you see Connected, or go back and fix your problem.

Do not proceed until you get a good connection. After you get a good connection, you may close the two files you downloaded from Nord.

Set up a NordVPN interface

This seems strange, but the fact is that the firewall rules are easily configured using an interface. There are likely people who can set this up without doing it, but we'll do it the easy way. We're going to create a fake *interface* that is associated with the NordVPN service

1. Go to **Interfaces** | **Assignments**
2. Under **Assign a new interface**, click the dropdown to select the one that says *OpenVPN Client NordVPN*
3. Under Description, choose **Nord** or **Nord IF**. Something you can find easily
4. Click the Add button
5. Click the new Nord interface (either from the list, or from the menu)
6. Ensure **Enable** is checked
7. Click **Save**

Create an Outbound NAT entry

This will allow traffic going out on the Nord interface (the NordVPN instance) to handle multiple connections and be correctly translated so, when the data returns, the router will know where to send

it.

1. **Firewall** | **NAT** | **Outbound**
2. Assuming **Mode** is set to Automatic, change it to **Hybrid**
3. Add new Manual rule by clicking the plus sign
    1. Name: Nord
    2. TCP/IP Version: IPv4
    3. Protocol: any
    4. Source Address: Lan net
    5. Translation Target: Interface address
    6. Category: OpenVPN
    7. Description: NAT Traffic from LAN through Nord
    8. Leave everything else blank
4. Click orange **Save** button

Force all LAN traffic through Nord

This is the final step. It will force all LAN traffic through the NordVPN connection by adding a rule in the LAN firewall. Once this rule matches, no other processing will occur, so any rules that supercede this should be placed physically before this rule

1. **Firewall** | **Rules** | **LAN**
2. Add new rule by pressing the orange +
    1. Action: Pass
    2. Quick: Checked (apply immediately)
    3. Interface: LAN
    4. Direction: in
    5. TCP/IP Version: IPv4
    6. Protcol: any
    7. Source: Lan net
    8. Log: check if you want to see what is happening, uncheck to save disk space
    9. Category: ovpn
    10. Description: Everything else goes through NORD
    11. Gateway: NORD_VPNV4 (the VPNV4 was added automagically when you defined your Nord interface)
3. Click orange **Save** button
4. Click **Apply Changes**

At this point, all LAN traffic should go through the NordVPN. A simple way to check is to open a web browser to https://www.whatsmyip.org/ and see that it is different from your WAN IP (which you saw before we started)

To perform split tunnelling, where some traffic goes through nordVPN and other traffic goes through other services, see opnSense + NordVPN + otherVPN

From:
https://kb.unixservertech.com/ - **Unix Server Tech Knowledge Base**

Permanent link:
https://kb.unixservertech.com/other/networking/opnsense/nordvpn

Last update: **2025/07/12 06:23**