opnSense + NordVPN + otherVPN

This document assumes you have a working NordVPN instance which handles all network traffic from your LAN. This is described in the article NORD VPN on opnSense

It also assumes you have a second VPN connection already created, and you want to route some traffic through that, with the NordVPN being the default for everything else (aka *Split Tunnel*)

We'll call the NordVPN instance **NordVPN** and the other instance **OfficeVPN**. The goal is to send all office related traffic through the **OfficeVPN** and everything else through the **NordVPN**.

Summary

Basically, for each instance, we need to

1. Create an alias containing all IP subnets you want handled
2. Set up new interface
3. Create Outbound NAT entry to correctly NAT LAN traffic destined
4. Create a firewall rule to force LAN traffic destined for subnets

For the default instance (NordVPN in this case), we use **any** instead of the aliased subnets.

Note: this assumes we are only interested in traffic originating from the LAN. It is possible we could build **Floating** rules to allow, for example, LAN and Wireles to do the same thing. That is not tested at this time.

Note: one of our routers has Multi-WAN for network failover. Tests so far show that the VPN instances hang when switching from one WAN to another. Further testing needed.

Create second tunnel

Ok, we assume the NordVPN is set up and running, and all traffic is going through it. Now, we want to create a second (or third, or fourth) path for traffic to take.

Alias target subnets

Find all target subnets. In this case, look at all subnets accessed through the **OfficeVPN**. A simple way is to edit the definition for the Site-To-Site VPN and look at all subnets. In my case, I chose:

- Remote Server: The public IP of the VPN server
- IPv4 Tunnel Network
- Everything in the IPv4 Remote Network entry

Procedure

1. **Firewall** | **Aliases**
2. Create new alias by pressing the orange Plus sign
    1. Enabled: checked
    2. Name: Office_Subnets
    3. Type: Networks
    4. Categories: openvpn
    5. Content: list every subnet, separated by commas. For a single IP, use a /32 at the end.
    6. Description: All networks for OfficeVPN

Create new interface

1. **Interfaces** | **Assignments**
2. Under Assign a new interface, select the Device. It will have *Client* and the VPN name in it
3. Description: Office (or OfficeVPN, or OfficeInterface, or whatever)
4. Click the **Add** button
5. Select the new interface, either from the menu on the left, or from the Assiments list
6. Ensure the interface is enabled.

At this point, clicking **System** | **Gateways** | **Configuration** will show you two new gateways, one for IPV4 and one for IPV6.

Set up Outbound NAT

1. **Firewall** | **NAT** | **Outbound**
2. Should be in **Hybrid** mode if you set the NordVPN (default) up
3. Add new Manual Rule by pressing the orange plus sign
4. Interface: OpenVPN
5. TCP/IP Version: IPv4
6. Source Address: Select the alias you created, ie *Office_Subnets*
7. Translation/target: Interface address
8. Click orange **Save** button
9. Ensure this rule precedes the Nord (default) rule. Not sure if this is necessary. If it does not preced it
    1. Place a check in the box by the new rule
    2. Click the left arrow to the right of the Nord rule
10. Click the **Apply Changes** button

Create firewall rule

The final step is to set up a firewall rule to route all traffic destined for the Office through the OfficeVPN interface. Following is set up to route the LAN traffic only (still working on other networks)

1. **Firewall** | **Rules** | ****LAN**
2. Add new rule by clicking the orange plus sign
    1. Action: Pass
    2. Quick: checked (apply action immediately)
    3. Interface: LAN
    4. Source: LAN net

5. Destination: Office_Subnets (hint, scroll UP to find aliases)
6. Category: OpenVPN
7. Description: Route Office VPN traffic through Office VPN
8. Gateway: Select **Office** or whatever you called the new interface from the dropdown

3. Click orange **Save** button
4. Move this rule **before** the NordVPN rule
    1. Place a check in the new rule
    2. Click the left facing arrow (on right) on the rule for the Nord entry
    3. Rule should move to just before the Nord entry
5. Click **Apply Changes** button

Summary

I'm not sure how to verify it is all working. I'm sure Insight/NetFlow could probably give some information. I would suggest first pinging something in the Office network and verify it works. Assuming it does, stop all activity on public IP's, then look at the VPN statistics. Now, copy something over to the Office. You should see the OfficeVPN stats increase fast, and the NordVPN stats stay fairly stable.

System | **Routes** | **Status** will show you the routing table. In my case, the first entry was everything, 0.0.0.0/1, going through the Nord connection, but the Office subnet was going through the OfficcVPN connection.

Anyway, if anyone has an idea, let me know. Just go to https://dailydata.net and click the Contact Us link.