Access N2N node from Road Warrior

With OpenVPN, you can have one router connected to another via a “Net-to-Net” (N2N) connection. This connection is established at startup (generally) and is maintained at all times (as long as both routers are on), connecting both networks over an encrypted connection. This is commonly used to connect branch offices which may be geographically separated.

“Road Warrior” VPN connections are designed to connect a single machine to a network instead of connecting two networks.

In some cases, you would like a Road Warrior connection to have access to a remote network over an N2N. One example would be giving technical support access to a branch office only through a Road Warrior connection to the main office. Tech Support then would only have access to a single network (the home office), but through it, could then access branch offices.

Assumptions

IP/Subnet	Definition
192.168.5.0/24	OpenVPN Subnet of Road Warrior Connections
192.168.6.0/24	LAN subnet on client site
192.168.7.0/30	Subnet of N2N connection
192.168.7.2	IP Address of Server's side of N2N Connection

You're road warrior connection targets same firewall as your N2N server (it should work with a few changes going into the N2N remote)

Theory

You not only need to add a route for the Road Warrior connections (to the remote node), but the remote node needs to know how to respond. Basic steps are:

1. Central (main) VPN server pushes N2N node's network to Road Warrior clients
2. Central (main) VPN server pushes Road Warrior's Tunnel Network to N2N node(s)
3. A firewall rule is created to allow traffic from ovpn to N2N Node network (may not be necessary)

Steps

- On Centeral (main) router
    1. VPN | OpenVPN | Servers
        1. Record Tunnel Network for Road Warrior configuration
        2. Record IPV4 network for N2N configuration
    2. Edit N2N Configuration
        1. Add Road Warrior Tunnel Network to IPv4 Local Network (separate with comma)
        2. Save Configuration

3. Restart N2N server (actually, I think this is automatic)
3. Edit Road Warrior Configuration
    1. Add N2N Remote Node's network to IPv4 Local Network (separate with comma)
    2. Save Configuration (if you are connected via vpn, you will lose connection and have to reconnect)
4. Firewall | Rules | OpenVPN (may not need to do this)
    1. Add rule
        1. Action - Pass
        2. Interface - OpenVPN
        3. Destination - Single host or Network (put N2N Remote Nodes network as the network)
        4. Save
        5. Apply Changes

1. On remote node
    1. VPN | Clients | N2N Name
        1. Add Central Node Road Warrior tunnel to IPv4 Remote Network (comma separated)

It should eventually pick up the changes, but you can restart the OpenVPN servers on your main (master) node and on your remote node. You'll also need to reconnect any Road Warrior clients so they can acquire the correct routes.

Result

A Road Warrior user can now make a vpn connection to the main (master) router. At that point, they have access to all machines on the remote node(s) also. If you have more than one remote node, you can perform the procedure multiple times to allow access to as many as you want.

Note: for security, you can set up a second RoadWarrior server for “normal” users (access only to the main network), and one that is setup for access to one or more remote nodes for Technicians, for example.

From:
https://wiki.linuxservertech.com/ - **Unix Server Tech Knowledge Base**

Permanent link:
https://wiki.linuxservertech.com/other/networking/opnsense/accessnodefromrw

Last update: **2022/12/16 23:22**