Multiple External WAN connections

Occasionally, you need more than one external network connections. If one outside (WAN, Internet, whatever you want to call it) fails, your router should automatically swap to a second.

OpnSense has done an excellent job of setting this up.

This is just a recipe. If you want to know what is going on, RTFM at Deciso (the authors). It is a good document with a lot of detailed information, including how to change the sensitivity (go up/down more/less often), using load balancing, and other things.

Anyway, here is my “quick and dirty”

My Scenario

Using a Protectli (https://protectli.com/) Vault with 4 ports

- WAN Port - Connected to Internet Provider via their modem (or their router in pass-through mode)
- LAN Port - My LAN
- OPT1 Port - Connected to a GL-iNet Puli Cellular Router with T-Mobile sim card
- OPT2 Port - Wireless Access Point (separate subnet). I am not setting this up in this document

Preparation

- Choose a separate Monitor IP for each WAN connection. In my case, I'm using 9.9.9.9 for the primary WAN, and 1.1.1.1 for the failover, but it can be any two reliable targets. Google at 8.8.8.8 and 8.8.4.4 is good.
- If you are doing any N2N (site-to-site) VPN's from your router, collect the subnet range for all targets, in other words, all of the remote LAN's you connect to over the VPN. **Hint**: Open each VPN connection and just copy the ranges from there.

Mess with Gateways

1. Add monitor IP's
    1. System | Gateways | Configuration
    2. For each gateway
        1. Disable Gateway Monitoring: UNCHECK
        2. Monitor IP: enter the IP you chose for this gateway
        3. Mark Gateway Down: UNCHECK
        4. Save
    3. When done, you should see all columns filled in, RTT, RTTd, Loss
2. Set up Gateway Group
    1. System | Gateways | Group
    2. Add Group
    3. Name: WANGROUP

4. set the primary gateway to be Tier1
5. Set the secondary to be Tier2
6. Set Trigger Level to be Packet Loss
7. Put in a description like Failover Group
8. Save

Set up separate DNS for each

- System | Settings | General
- For each gateway
  - Enter one or more separate DNS server
  - They must NOT be the same, for some reason
- Check *Default Gateway Switching* if using Unbound for DNS

Firewall Rules

1. Create VPN Alias (only if you have router based N2N VPN)
   1. Firewall | Alias
   2. New Alias (Plus sign)
   3. Name: vpn_subnets
   4. Type: Network(s)
   5. Categories: MultiWAN
   6. Content: put all remote VPN subnets, hint, separate with comma's, example, 192.168.1.0/24,10.10.10.0/23
   7. Description: All remote VPN networks we access
   8. Save
2. Firewall | Rules | LAN
   1. IF you are setting up for VPN
      1. Clone rule which has description “Default allow LAN to any rule”
      2. Change Gateway to the gateway group you defined (*WANGROUP* in these instructions)
      3. Change description by appending “Modified ” (so you can tell which one you changed)
      4. Save
      5. Go to original rule (above the one you just changed, we hope). This must be before the “Modified” one in the list
      6. Change Destination to the alias you created before (vpn_subnets)
      7. Change Description to something like “Route VPN traffic through default gateway”
      8. Save
   2. If you are NOT setting up for VPN
      1. Edit rule which has a description of “Default allow LAN to any rule”
      2. Change gateway to the gateway group you defined (*WANGROUP* in these instructions)
   3. Add a new firewall rule **above** the one or two you have created here
      1. Action: Pass
      2. Interface: LAN
      3. TCP/IP Version: ipv4
      4. Protocol: TCP/UDP
      5. Source: Any

6. Destination: Single host or network
7. Destination: your LAN IP of the router, ie 192.168.1.1/32
8. Destination Port Range: DNS - DNS
9. Category: DNS
10. Description: Local Route DNS
11. Gateway: Default
12. Save

4. Apply Changes

Testing

1. Open a window and start pinging something.
2. Open your routers WebUI
    1. Reports | Traffic
    2. Ensure both WAN and Failover WAN are on (I turn off LAN for this so I can see what is going on)
3. Shut down the primary WAN (I'm lazy, so I just unplug the network cable)
    1. You may see your ping's skip a few numbers.
    2. You'll see the WAN traffic die, to be picked up by the Failover WAN
    3. Run any additional tests
    4. **Note**: VPN may die, and it may take 15 seconds to a minute for the VPN connection to realize it has to reconnect. You can force restart the VPN connection to speed things up.
4. Bring your primary WAN back online
    1. Again, pings may skip a little
    2. You'll see Failover WAN's traffic die down and picked up by primary
    3. **Note**: your VPN connections will maintain on the failover WAN for a while. In my case, this will use up data on my Cellular Router, so I restart the connection manually to force the connection back to primary instead of waiting a minute or two.

Links

- https://docs.opnsense.org/manual/how-tos/multiwan.html
- https://docs.opnsense.org/manual/multiwan.html
- https://docs.opnsense.org/manual/gateways.html

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

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

Last update: **2024/12/15 08:12**