

SD-WAN NAT - PART II - Port Forwarding

In this article, I want to discuss the SD-WAN NAT feature.

A vEdge cloud router can play a NAT role. it can do the natting both on the transport side (VPN 0) and in the service side (VPN 1 for example).

If we deploy NAT in the transport side, NAT functionality allows traffic from the localhost to move directly to the Internet. We can do port forwarding.

The NAT software performs both address and port translation.

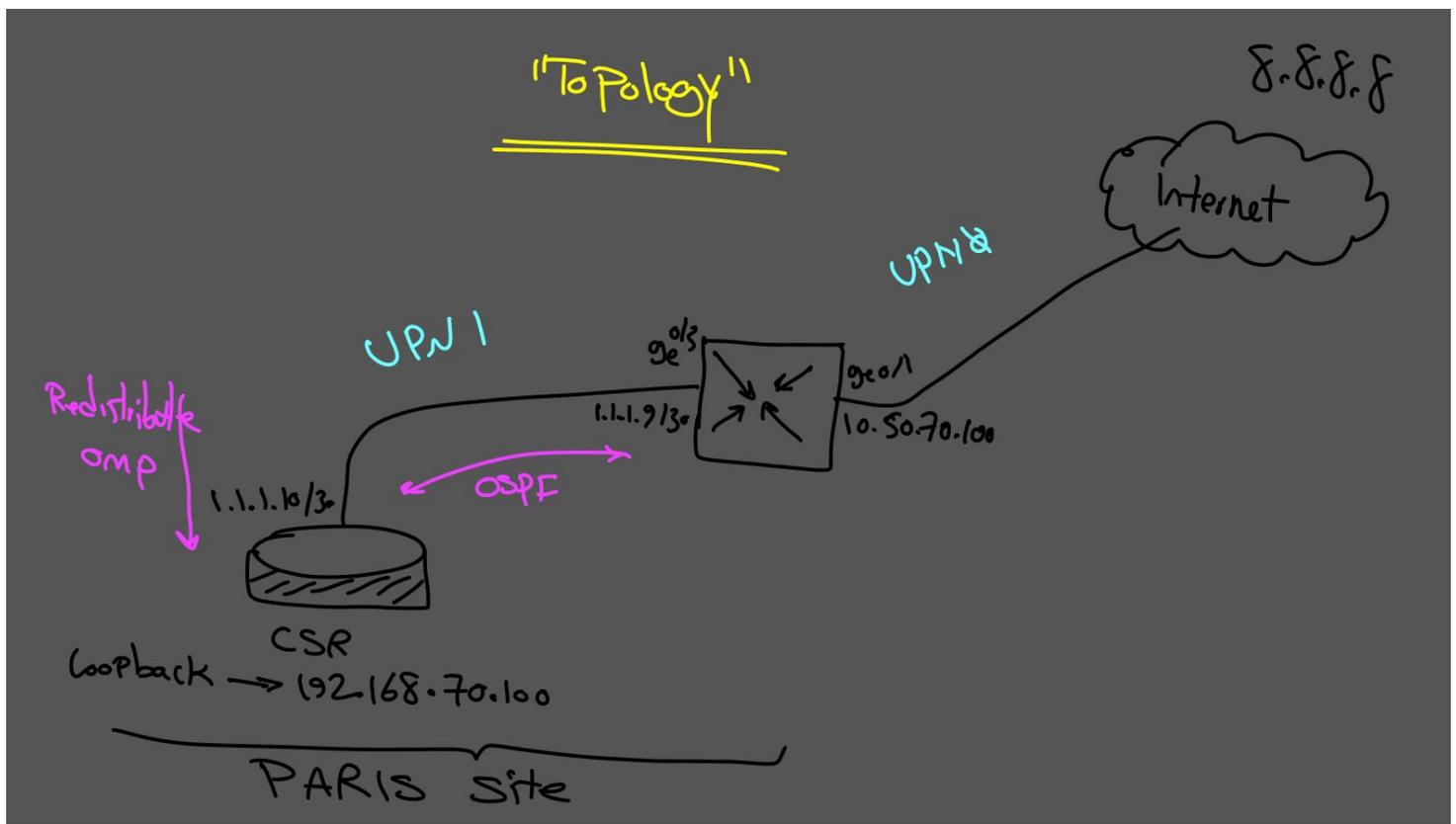
Cisco SD-WAN nat software supports 64,000 nat flows.

In this scenario, I want to do "**PORT FORWARDING**" on the transport side.

To achieve this goal, we need to do three critical steps.

- Enable NAT on an interface that faces public Internet in VPN 0 (in our scenario its ge0/1).
- Configure port forwarding.
- Direct traffic from service VPN like VPN 1 to go to the Internet (public) so we need to have a route to VPN 0.

In the last step, we need to do verification in vmanage.



Let's do configuration:

In my scenario, I am using vManage to do the configuration for Paris Site.

First, we go to "templates" menu.

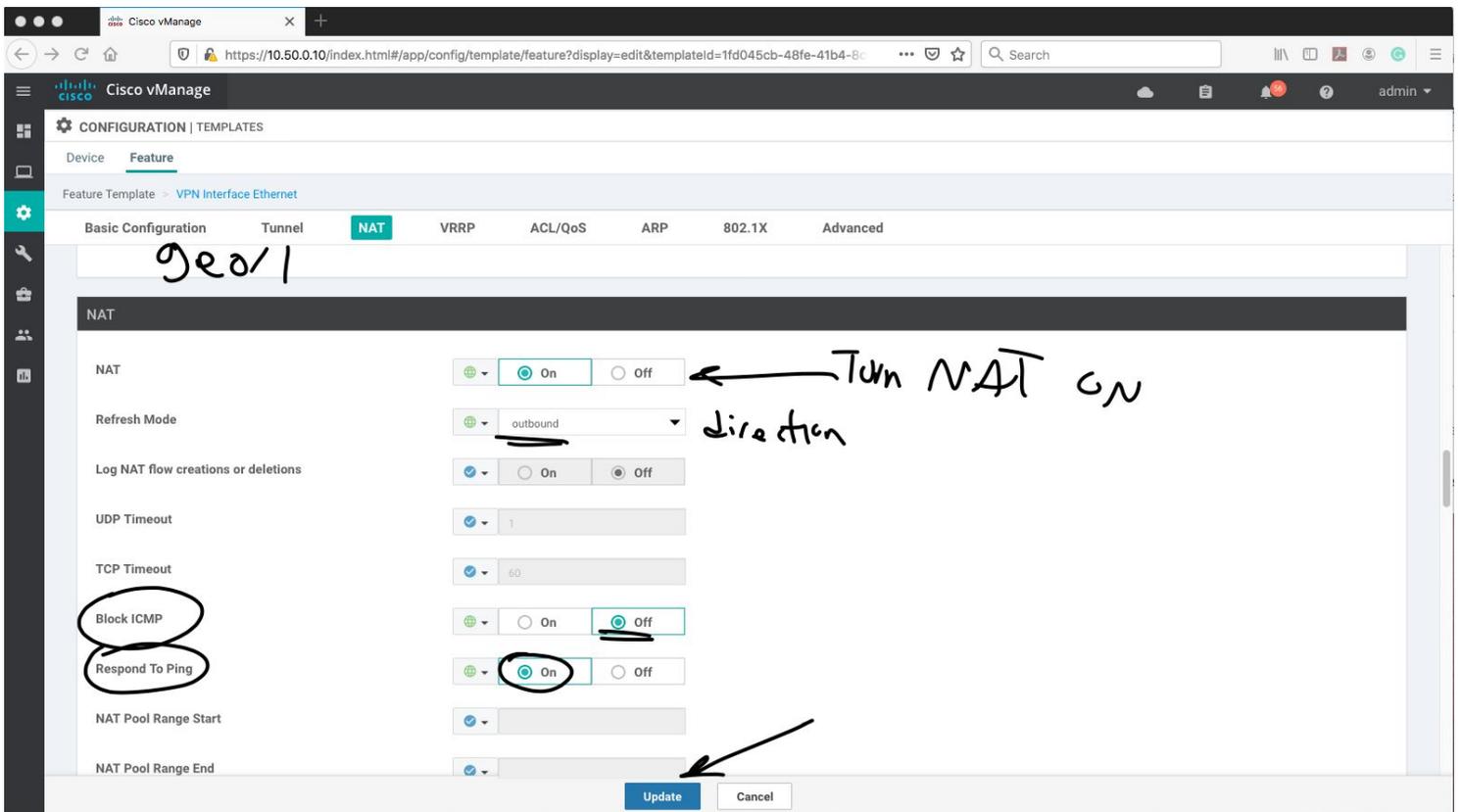
The screenshot shows the Cisco vManage dashboard. The left sidebar has a menu with 'Templates' highlighted. The main dashboard area contains several widgets: 'Site Health (Total 7)' showing connectivity status for 3, 4, and 0 sites; 'WAN Edge Health (Total 9)' with 9 Normal, 0 Warning, and 0 Error status; 'Transport Interface Distribution' showing utilization levels; 'Transport Health' with a line graph; 'Application-Aware Routing' table; and 'FireWall Enforcement' and 'Top Signature Hits' sections.

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
reykjavik.metro-ethernet-sanjose.metro-eth...	4.614	0.008	4.936
reykjavik.metro-ethernet-tokyo.metro-ethernet	6.1	0.007	6.55
reykjavik.metro-ethernet-toronto2.metro-eth...	6.236	0.007	6.6

The first step is to enable NAT on VPN0.

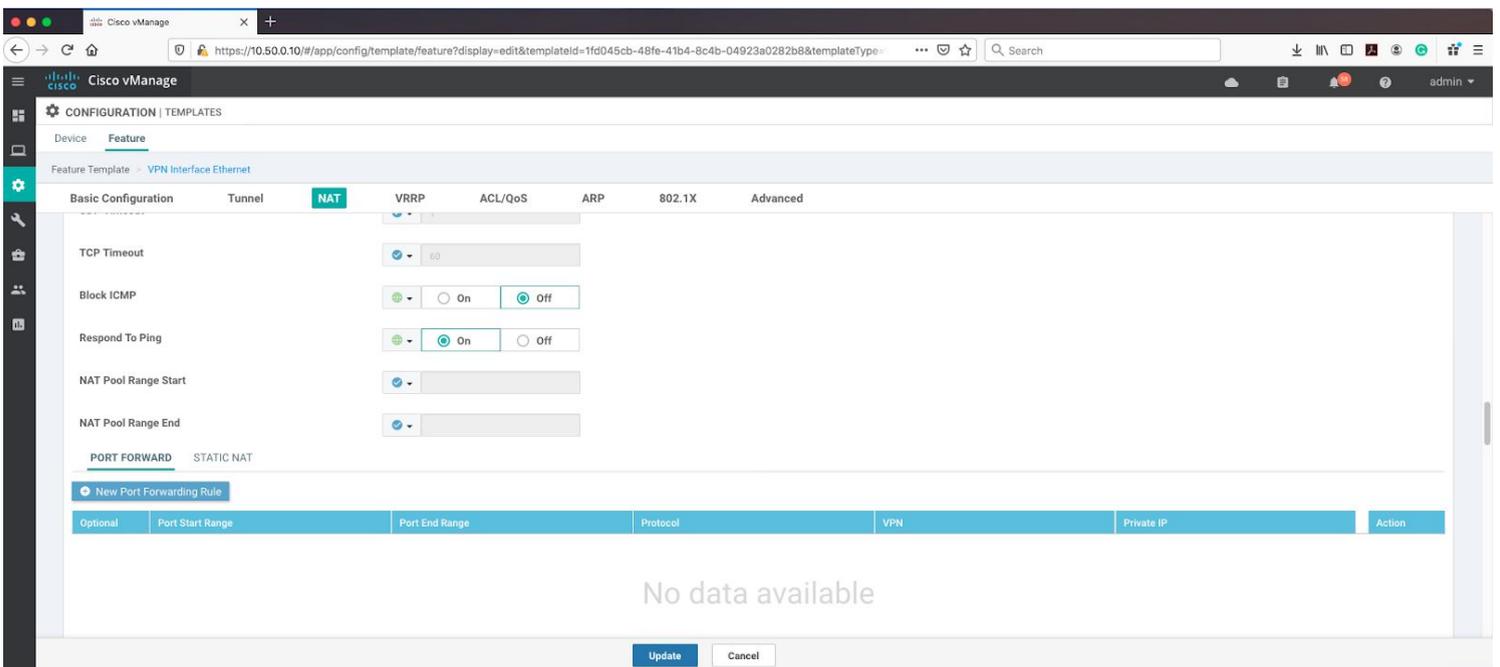
The screenshot shows the 'CONFIGURATION | TEMPLATES' page in Cisco vManage. The 'Transport & Management VPN' tab is selected. Under the 'VPN 0' section, the 'VPN Interface' dropdown is set to 'ge0/1-internet'. A handwritten note 'NAT must be enabled here!' with an arrow points to this dropdown. The 'Additional VPN 0 Templates' list includes BGP, OSPF, VPN Interface, VPN Interface GRE, VPN Interface IPsec, and VPN Interface PPP.

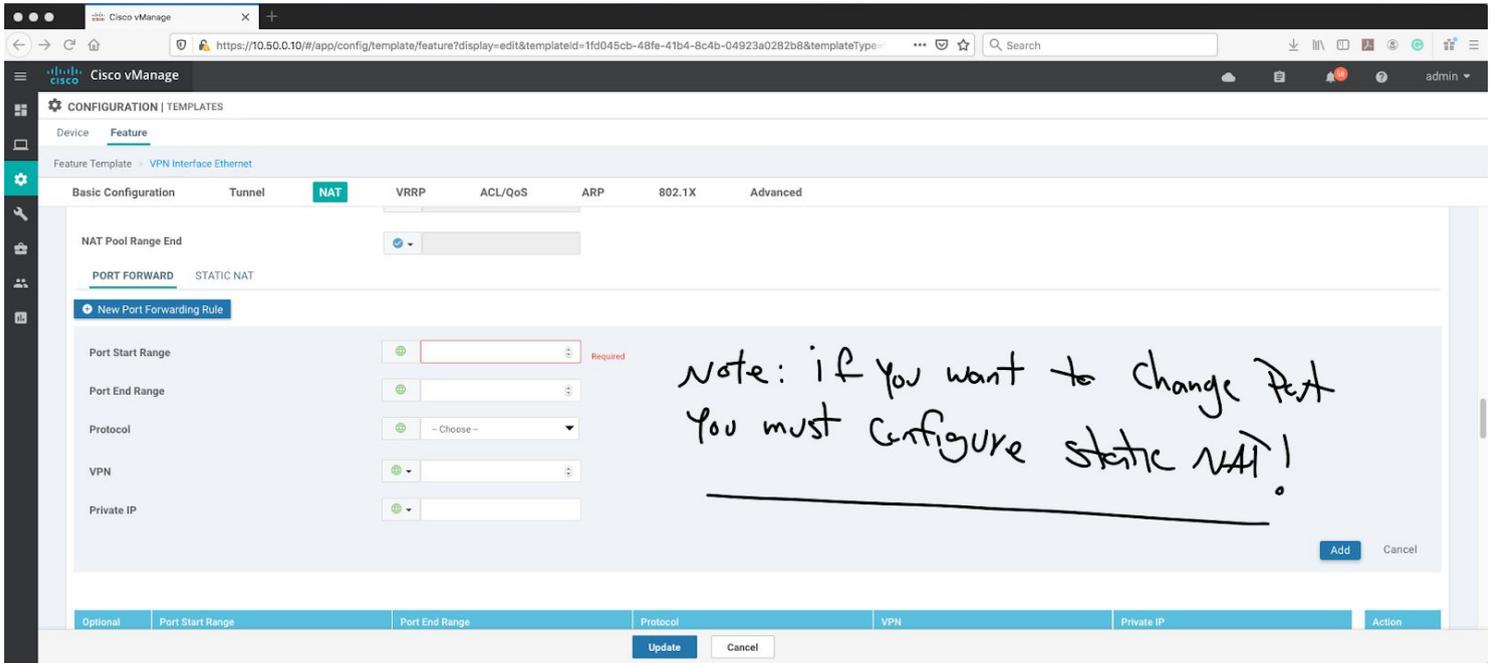
Under Interface, we configure the NAT feature.



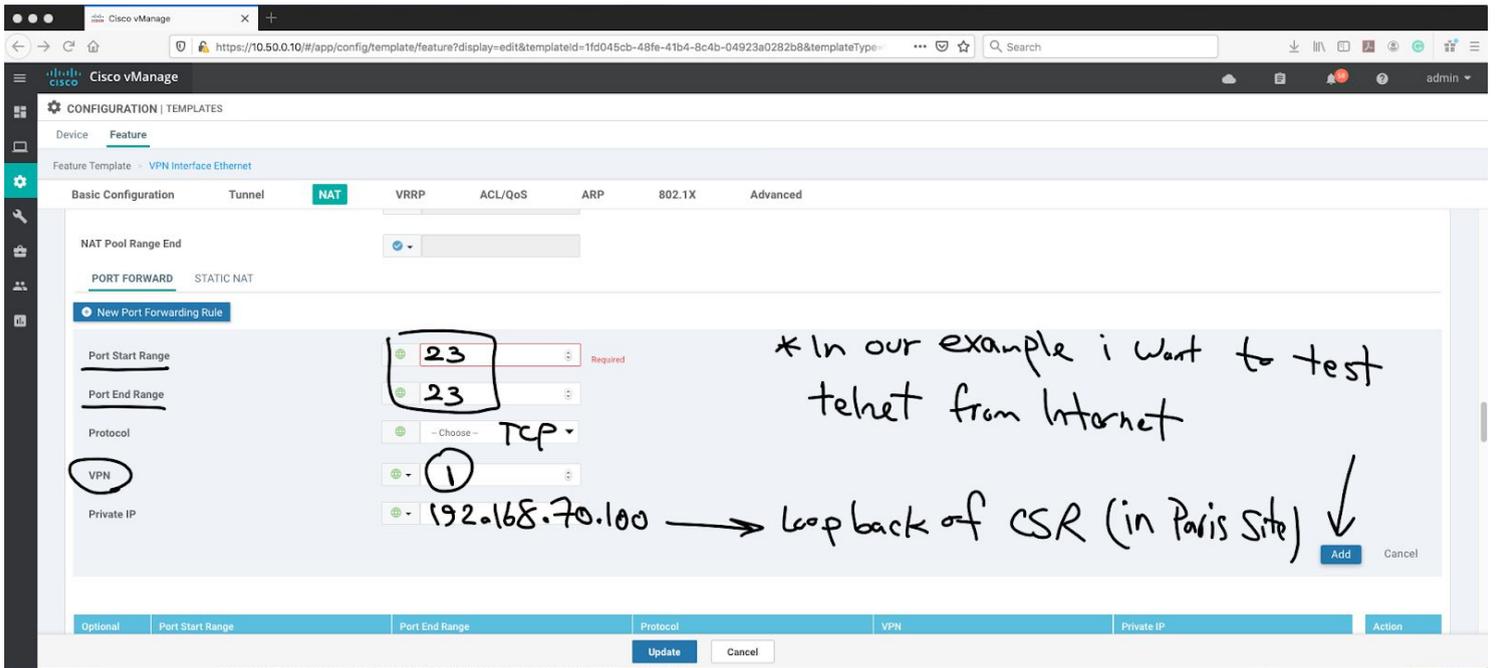
The second step is to configure "PORT FORWARDING" under Interface facing the public Internet.

Note: If you want to configure NAT port, then you must use STATIC NAT.



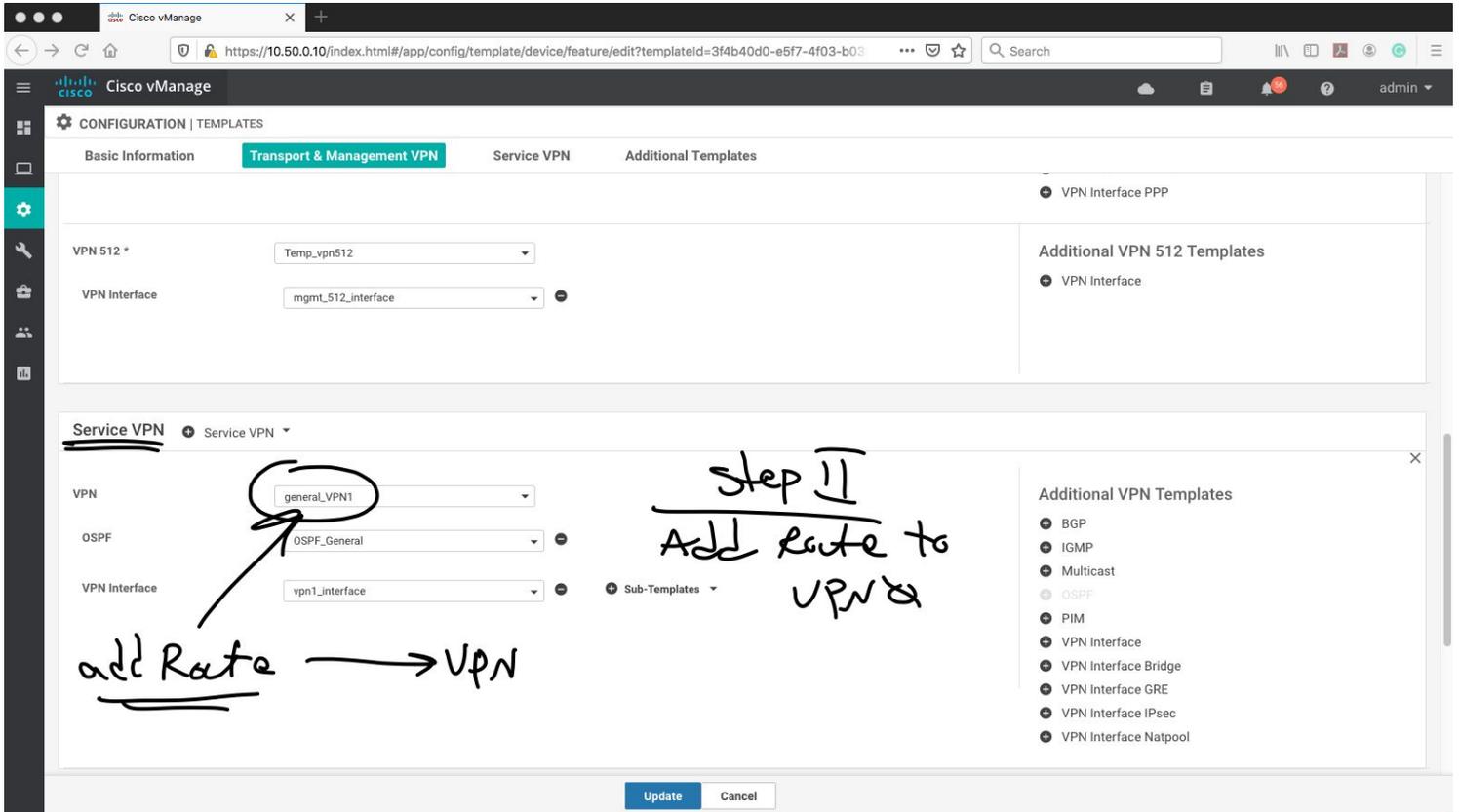


And here is the configuration for port forwarding.

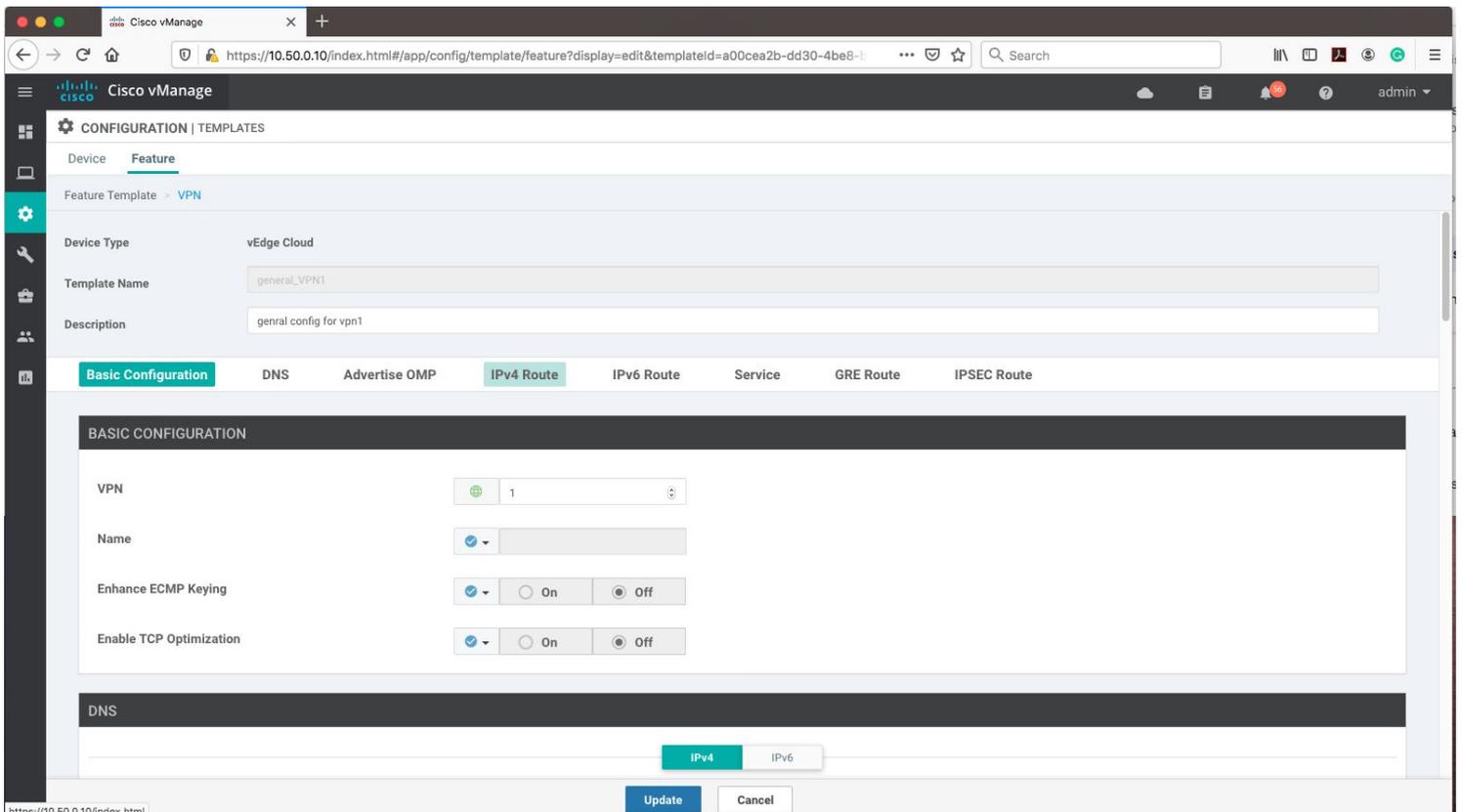


Let's do the third and final step.

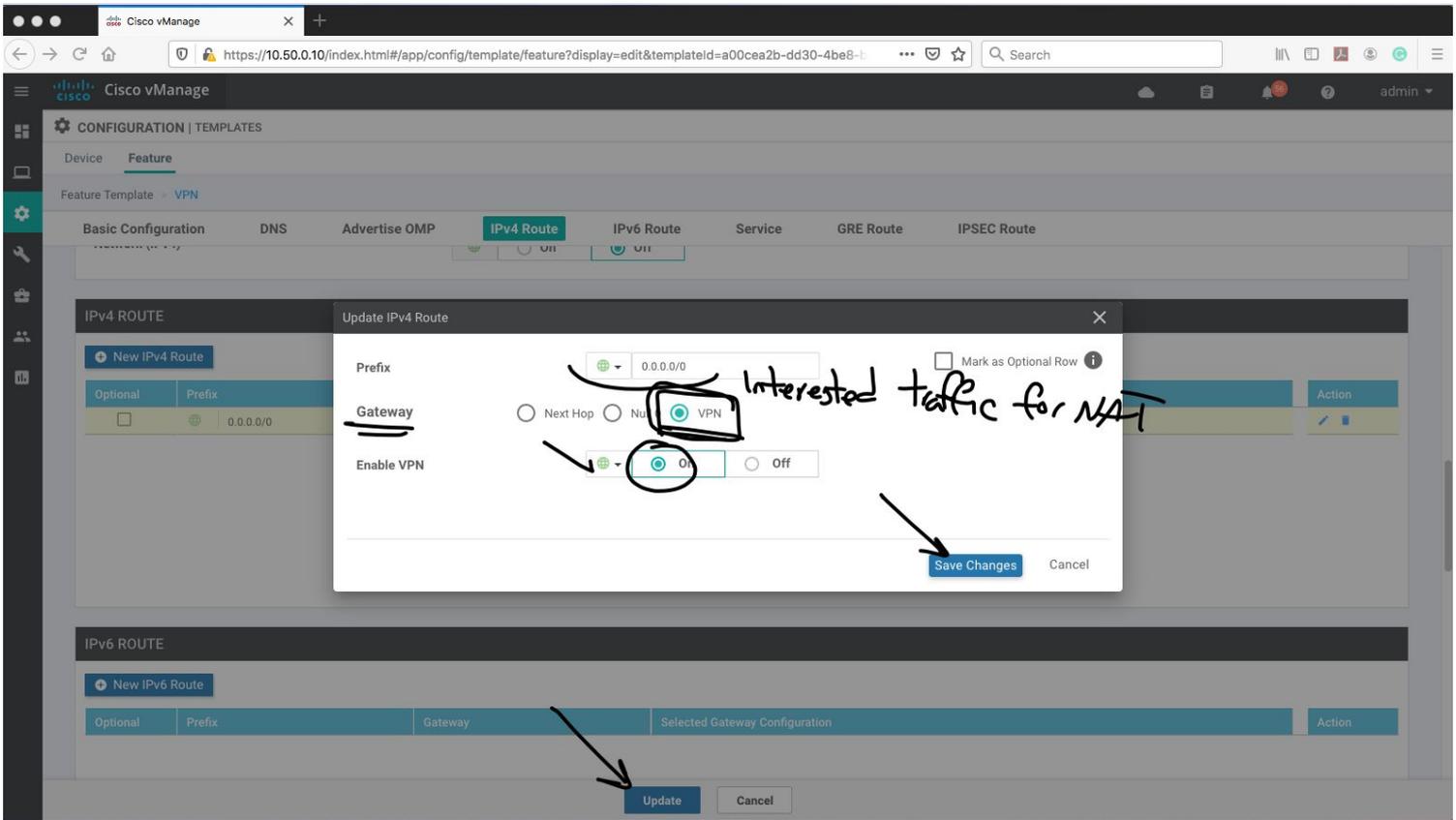
- In this step, we have to add a route in service side to VPN 0.



For this goal, first, we go to VPN 1(in our scenario service VPN is 1) template:

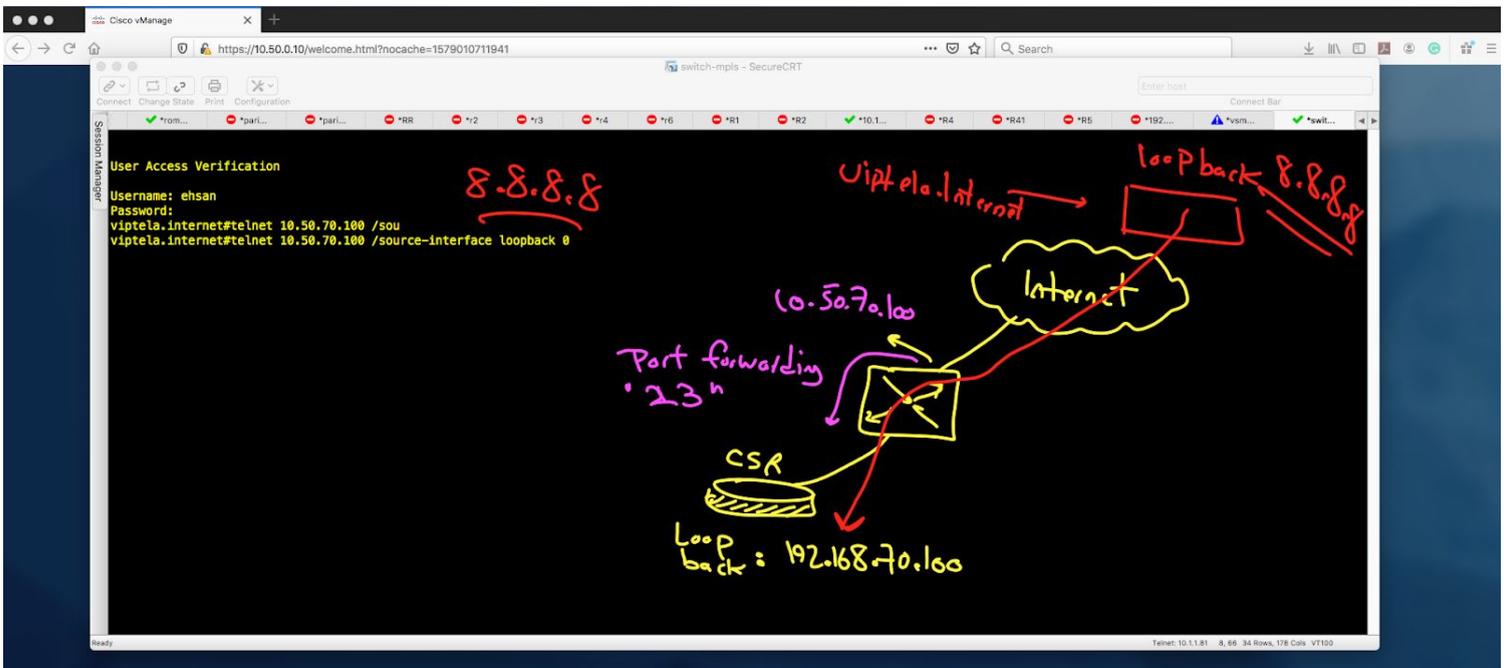


Note- Remember to choose interesting traffic for NAT.



Verification:

Now try to establish a TELNET session from Internet (simulated 8.8.8.8) to public IP of our vEdge IP address (10.50.70.100).



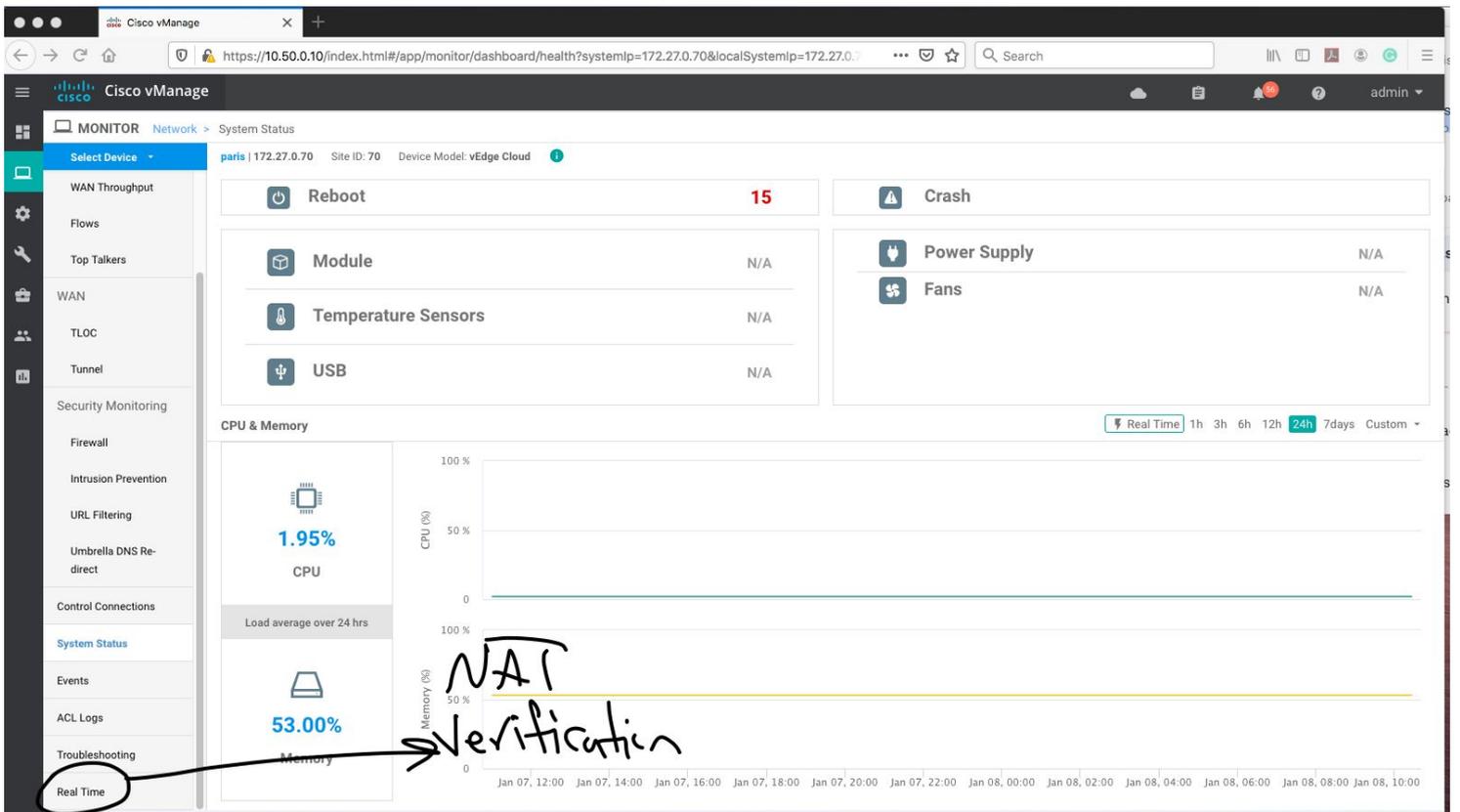
```

switch-mpls - SecureCRT
viptela.internet#
viptela.internet#telnet 10.50.70.100 /sour
viptela.internet#telnet 10.50.70.100 /source-interface loo
viptela.internet#telnet 10.50.70.100 /source-interface loopback 0
Trying 10.50.70.100 ... Open

User Access Verification
Username: admin
Password:
paris-csr#who
Line      User      Host(s)      Idle      Location
* 1 vty 0  admin    idle         00:00:00

```

For vManage verification follow the steps:



Device Options:

- IP NAT Interfaces
- IP NAT Filters
- IP NAT Statistics

Property	Value
Device groups	[No groups]
Domain ID	1
Hostname	paris
Last Updated	08 Jan 2020 10:35:37 AM EST
Latitude	37.666684
Longitude	-122.777023
Personality	Wan Edge
Site ID	70
Timezone	UTC
Vbond	10.50.1.1

Device Options:

Filter

Last Updated	NAT VPN ID	NAT If Name	VPN ID	Protocol	Private Source Address	Private Destination Address	Private Source Port	Public Source Address	Public Destination Address
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	icmp	10.50.70.100	10.50.1.1	17136	10.50.70.100	10.50.1.1
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	icmp	10.50.70.100	10.50.1.1	17225	10.50.70.100	10.50.1.1
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.1.1	12346	10.50.70.100	10.50.1.1
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.1.5	12346	10.50.70.100	10.50.1.5
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.1.10	12346	10.50.70.100	10.50.1.10
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.11.100	12346	10.50.70.100	10.50.11.100
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.21.100	12346	10.50.70.100	10.50.21.100
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.31.100	12346	10.50.70.100	10.50.31.100
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.35.100	12346	10.50.70.100	10.50.35.100
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.71.100	12346	10.50.70.100	10.50.71.100
14 Jan 2020 9:09:03 AM EST	0	ge0/1	0	udp	10.50.70.100	11.11.11.2	12346	10.50.70.100	11.11.11.2
14 Jan 2020 9:09:03 AM EST	0	ge0/1	1	tcp	<u>192.168.70.100</u>	<u>8.8.8.8</u>	<u>23</u>	<u>10.50.70.100</u>	<u>8.8.8.8</u>
14 Jan 2020 9:09:03 AM EST	0	ge0/1	1	udp	1.1.1.10	8.8.8.8	51742	10.50.70.100	8.8.8.8

Verified!

I hope you enjoy the article.

To be continued...