

SD-WAN NAT – PART I

In this article, I want to explain 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 on the service side (VPN 1 for example).

If we deploy NAT in the transport side, NAT functionality allows traffic from local host to move directly to the internet. We can do port forwarding or we can do dynamic PAT.

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 dynamic PAT on the transport side.

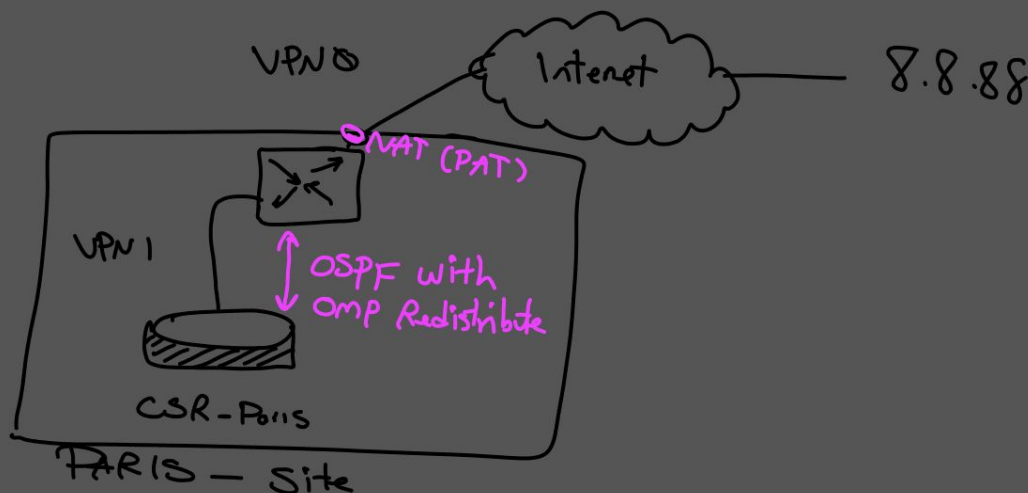
To achieve this goal, we need to do two critical steps.

1. Enable NAT on an interface that faces public internet in VPN 0 (in our scenario its ge0/1)
2. Direct traffic from other VPN like VPN 1 to go to the internet (public), we need to have a route to VPN 0

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

Direct Internet Access

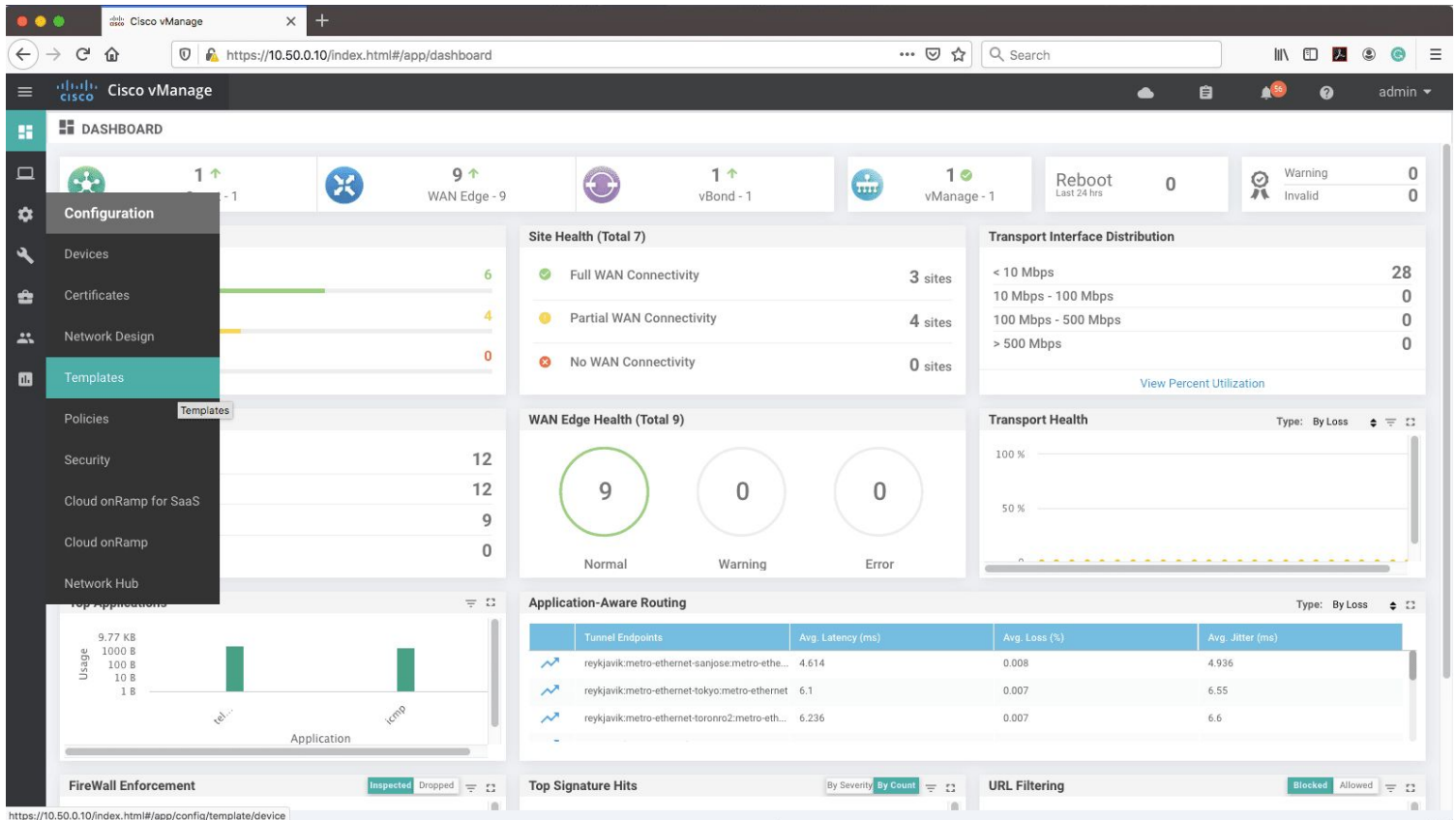
= NAT = "Transport VPN"



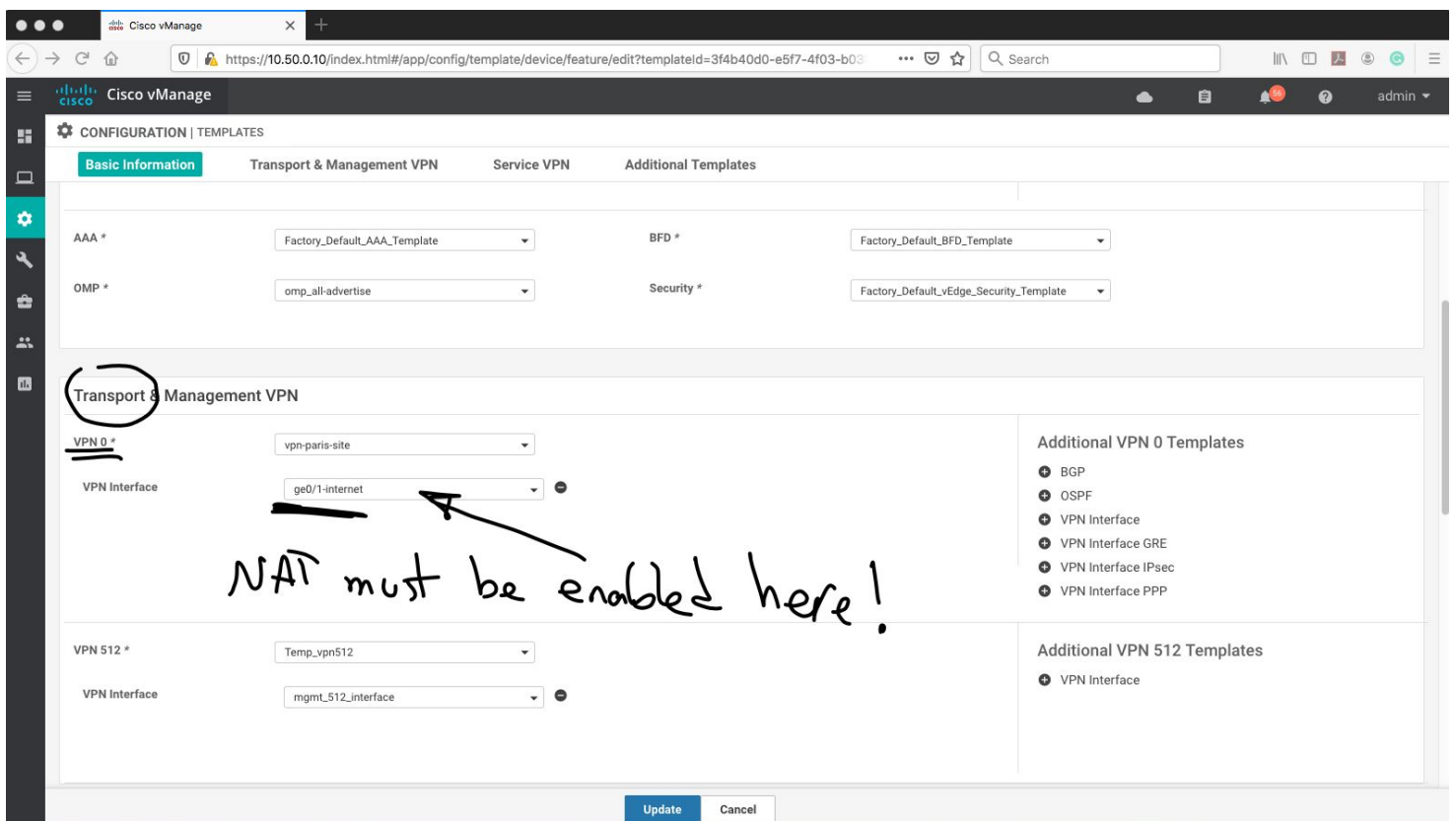
Let's do configuration

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

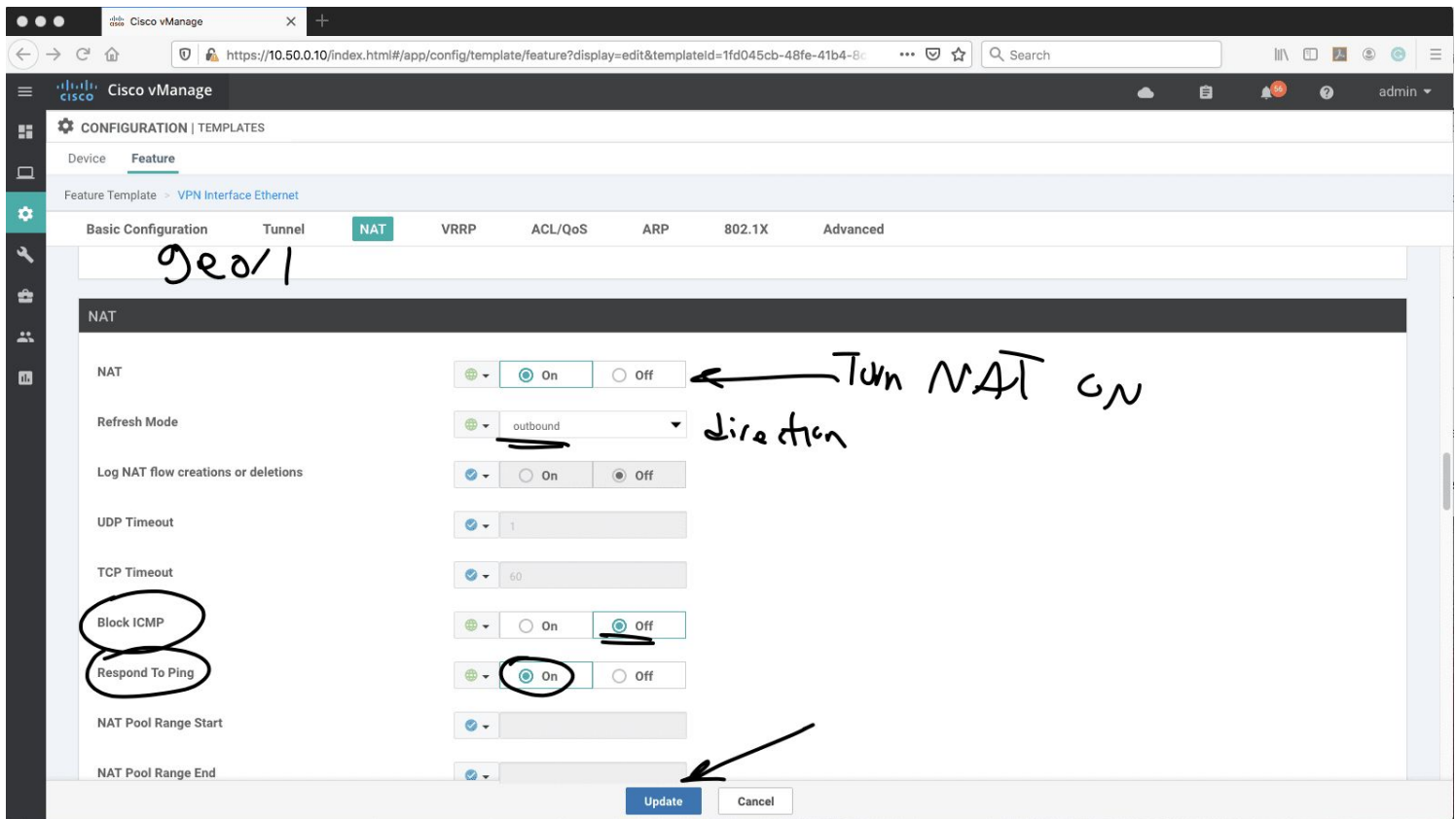
- First, we will go to "templates" menu.



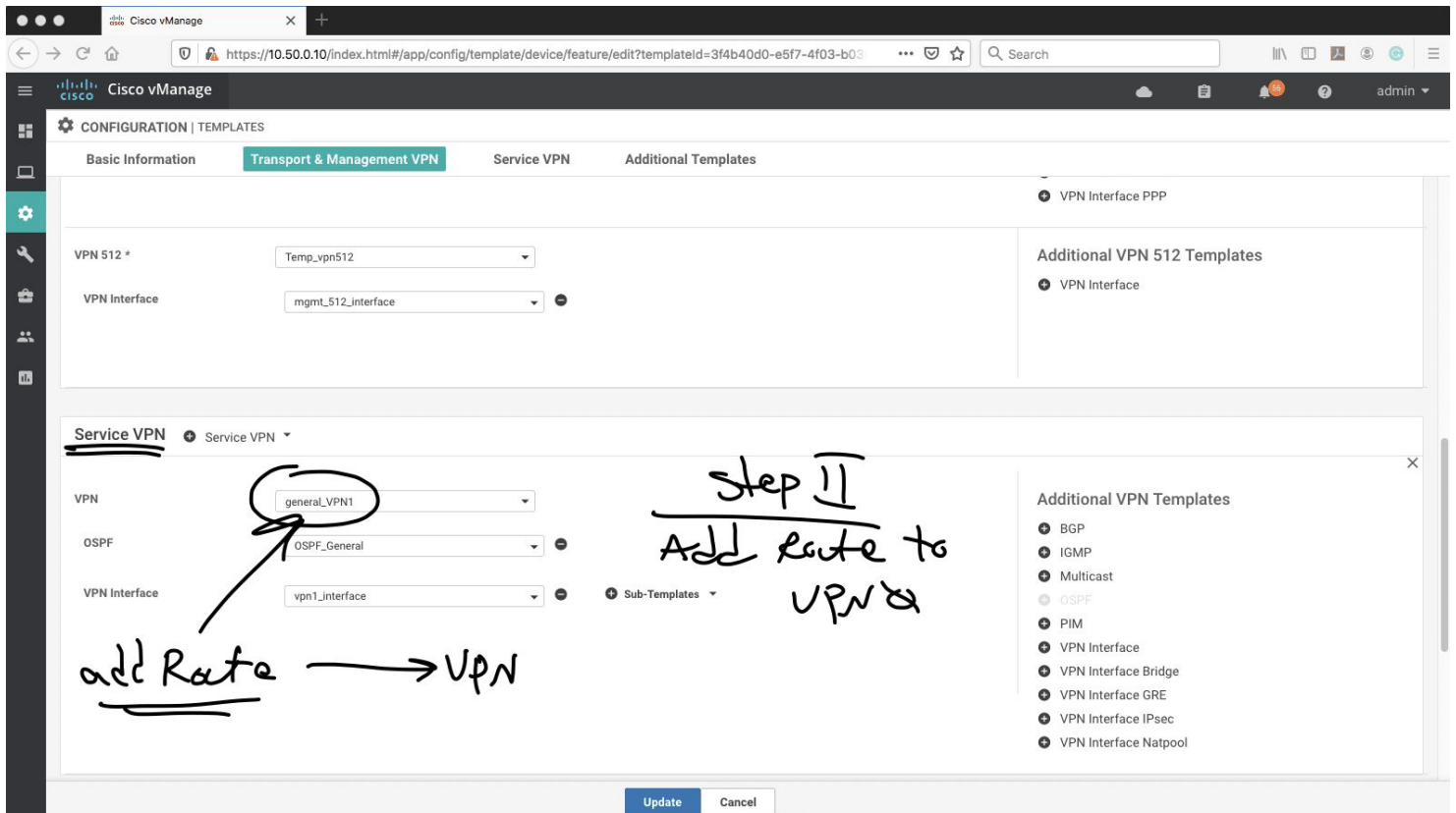
The next step is to enable NAT on VPN0, under interface facing the public internet.



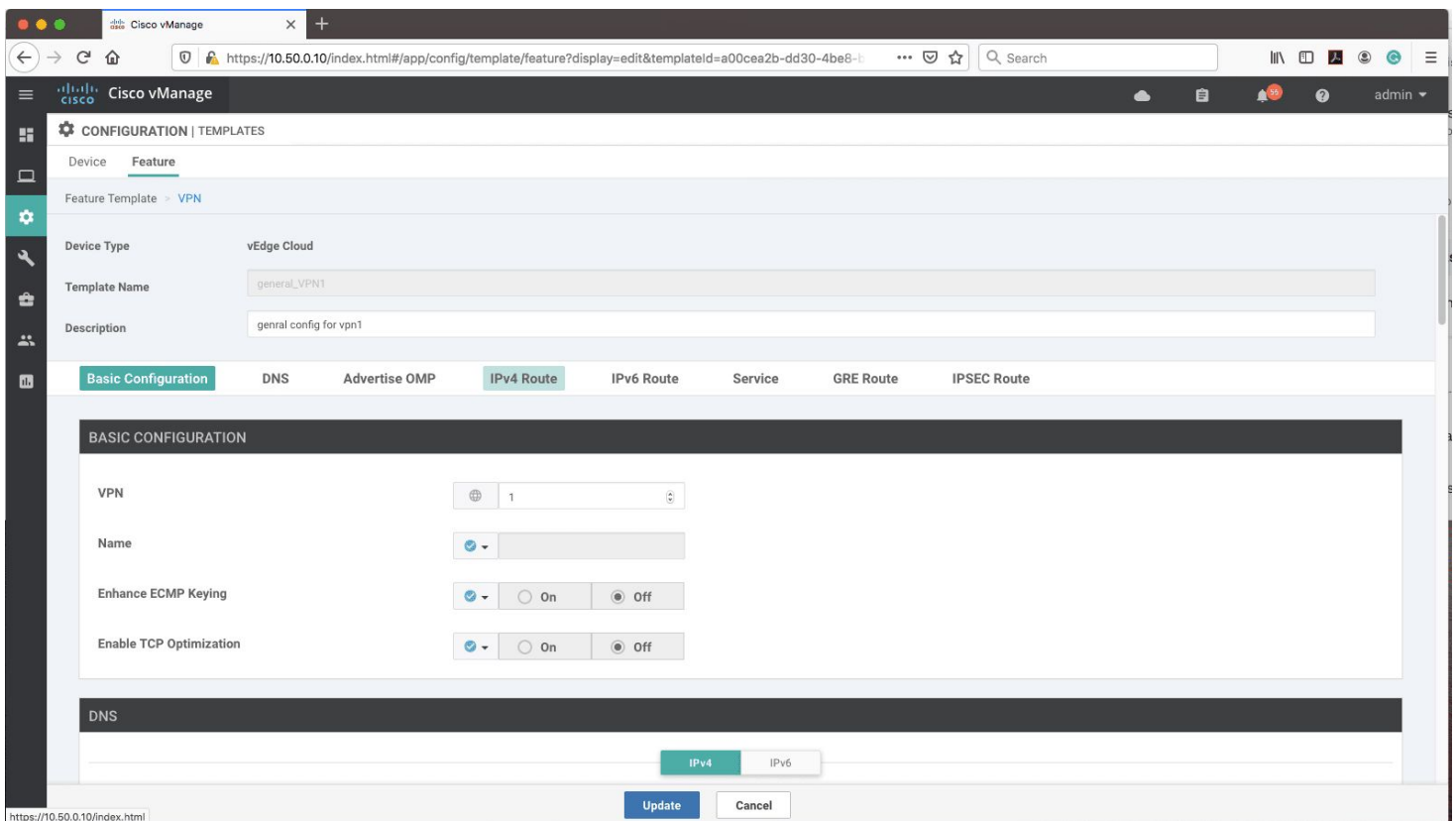
- Now under interface, we will activate the nat.



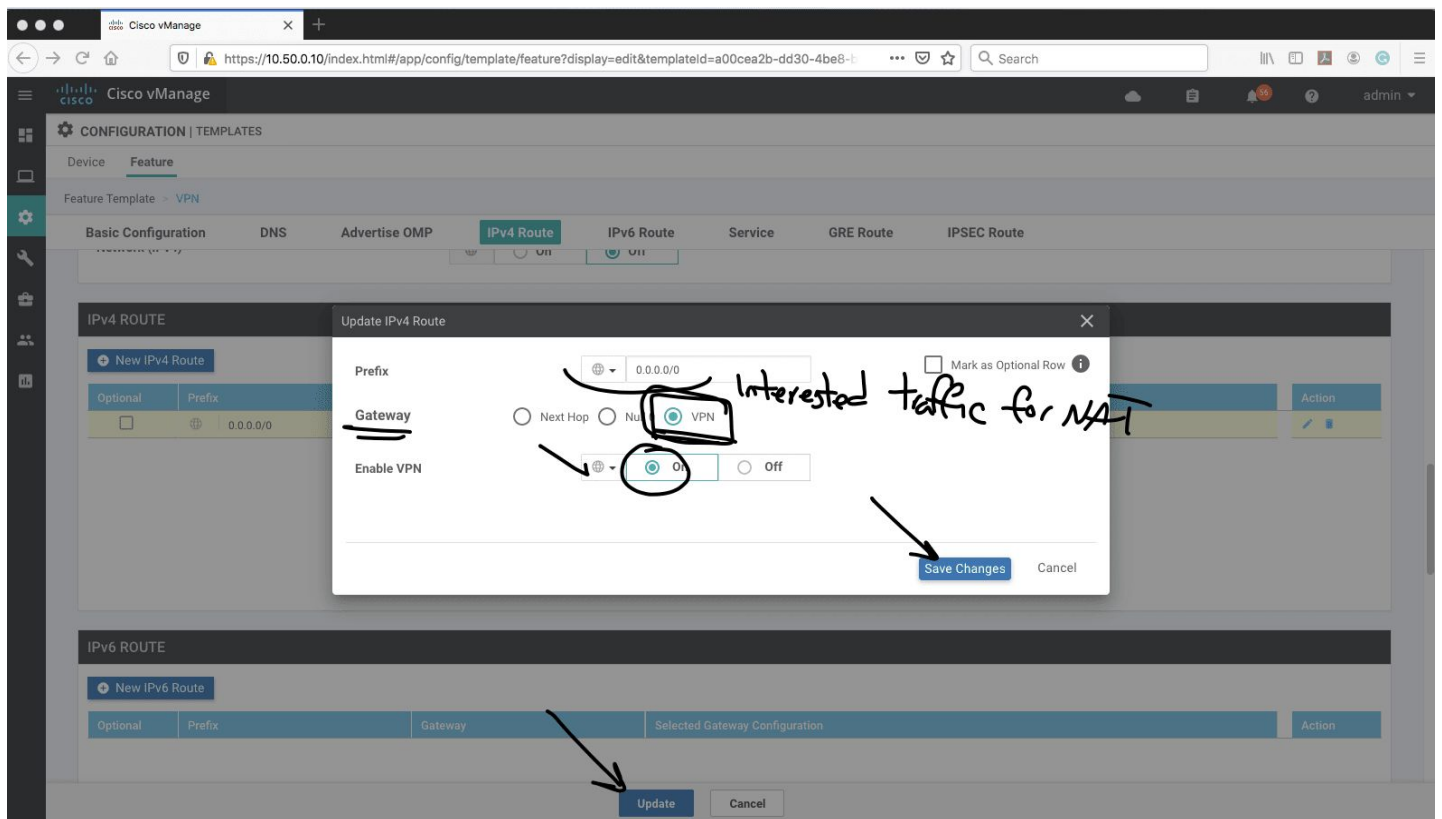
- Let's do the second step.
- In this step, we have to add a route in service side point to VPN 0.



- We go to VPN 1(in our scenario service VPN is 1) template



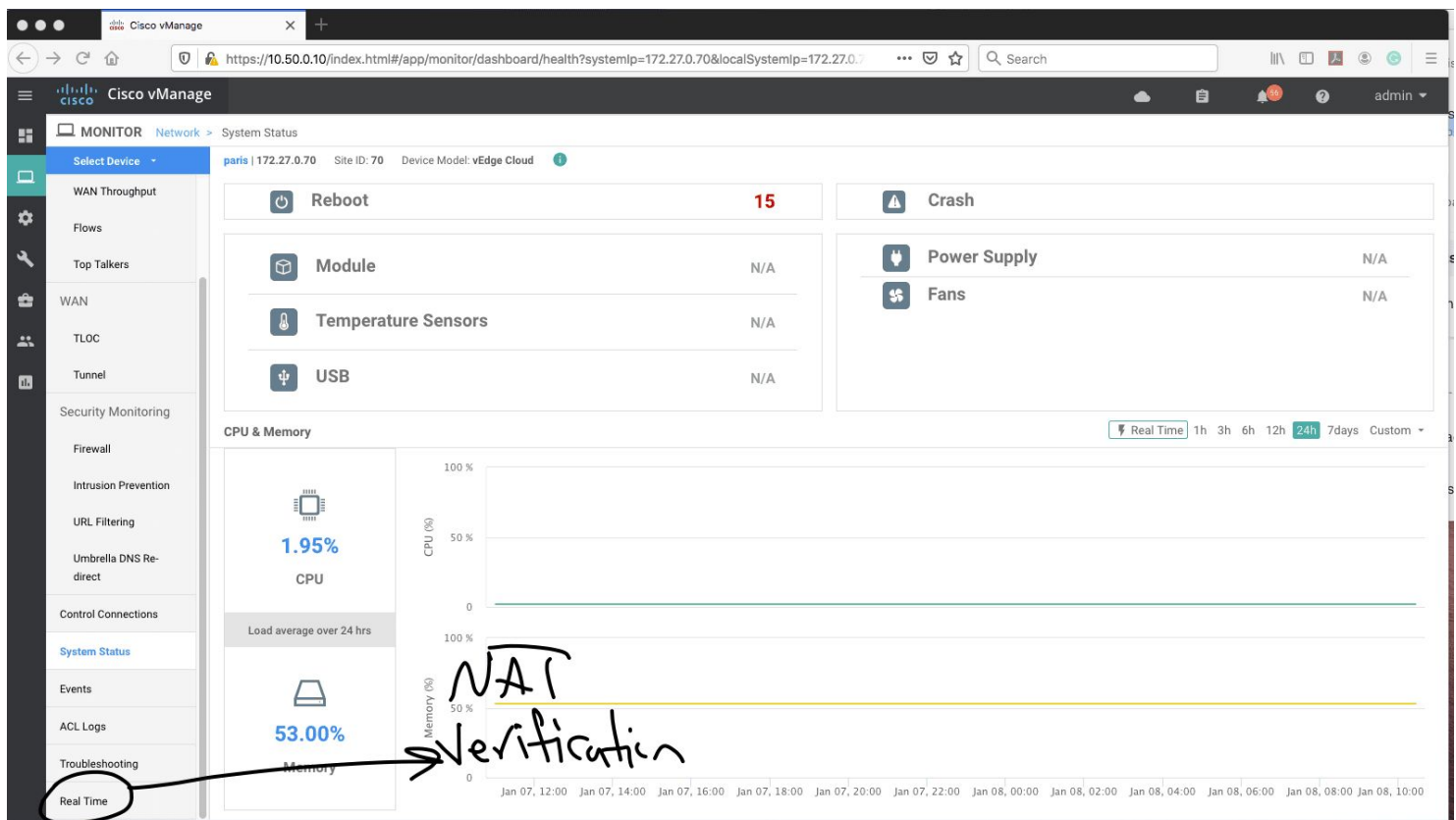
Note: remember to choose interesting traffic for NAT



- Now the ping from service side (CSR router) is going through internet



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

Total Rows: 10

Now I do another ping from loopback source to 8.8.8.8

```

paris-csr#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
paris-csr#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
paris-csr#ping 8.8.8.8 sou
paris-csr#ping 8.8.8.8 source 192.168.70.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.70.100
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
paris-csr#
paris-csr#
paris-csr#sh ip int br
paris-csr#sh ip int brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet1  10.50.0.170     YES NVRAM  up          up
GigabitEthernet2  1.1.1.10        YES NVRAM  up          up
Loopback1       192.168.70.100  YES NVRAM  up          up
paris-csr#
paris-csr#ping 8.8.8.8 sou
paris-csr#ping 8.8.8.8 source 192.168.70.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.70.100
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
paris-csr#

```


As you can see, real IP address is shown in vmanage and the configuration is verified.

The screenshot shows the Cisco vManage interface. The left sidebar contains navigation options: WAN Throughput, Flows, Top Talkers, WAN, TLOC, Tunnel, Security Monitoring, Firewall, Intrusion Prevention, URL Filtering, Umbrella DNS Redirect, Control Connections, System Status, Events, ACL Logs, Troubleshooting, and Real Time. The main content area is titled 'MONITOR Network > Real Time'. It shows details for 'paris | 172.27.0.70' and 'Device Model: vEdge Cloud'. A search bar for 'IP NAT Filters' is highlighted. Below it, a table displays NAT configuration details. The last row of the table is circled, showing a successful NAT translation for ICMP traffic from 10.50.70.100 to 192.168.70.100. Handwritten annotations include 'Verified!' and circles around the 'icmp' protocol, the private source address '10.50.70.100', and the public destination address '192.168.70.100'.

Last Updated	NAT VPN ID	NAT If Name	VPN ID	Protocol	Private Source Address	Private Destination Address	Private Source Port	Publ
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	icmp	10.50.70.100	10.50.1.1	14906	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	icmp	10.50.70.100	10.50.1.1	15014	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.1.1	12346	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.1.5	12346	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.1.10	12346	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.11.100	12346	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.21.100	12346	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.31.100	12346	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.35.100	12346	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	udp	10.50.70.100	10.50.71.100	12346	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	0	udp	10.50.70.100	11.11.11.2	12346	10.5i
08 Jan 2020 11:01:21 AM EST	0	ge0/1	1	icmp	10.50.70.100	192.168.70.100	26	10.5i

I hope you enjoy the article.
To be continued...