Cisco SD-WAN - Static NAT (PART III)

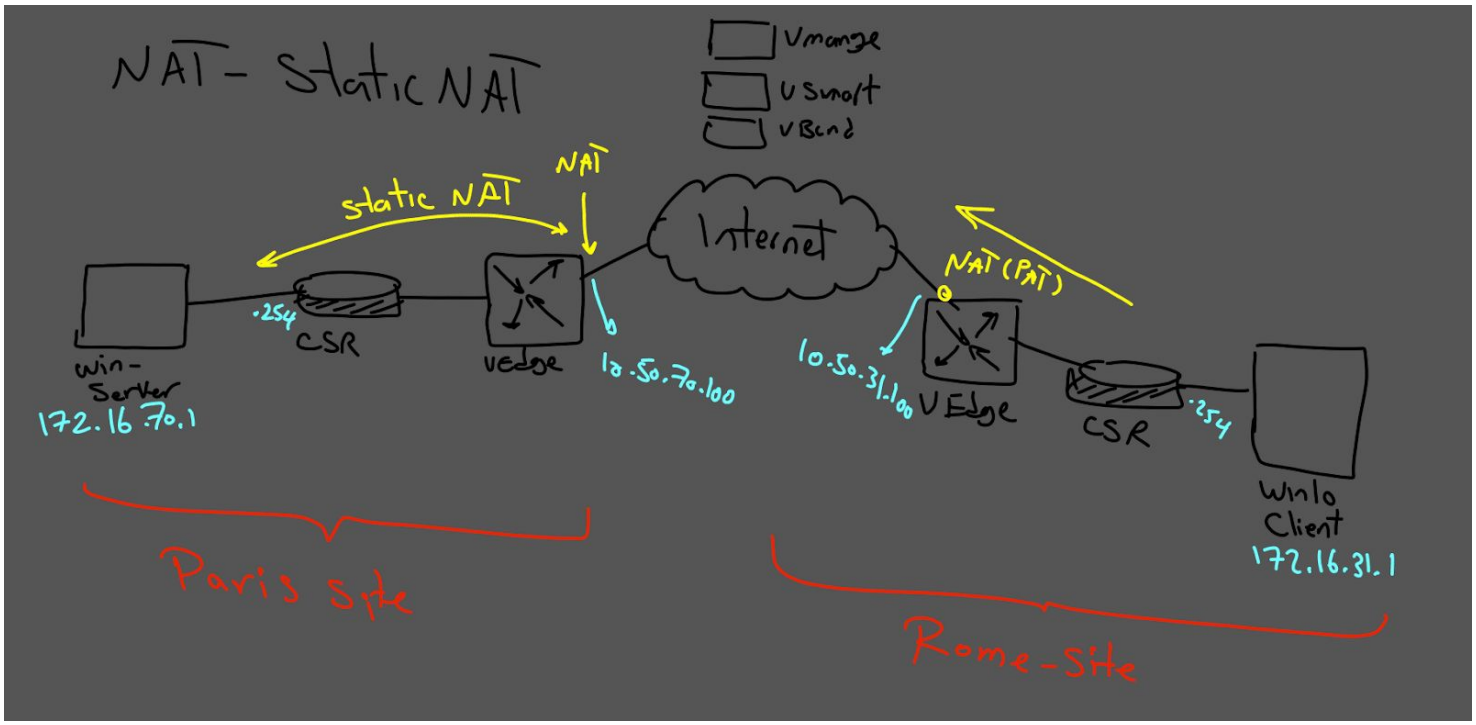
In this article, I want to discuss the SD-WAN "STATIC NAT" feature.
A vEdge cloud router can play a NAT role. It can do the natting both on the transport side (VPN 0) and on the service side (VPN 1, for example).

If we deploy NAT in the transport side, NAT functionality allows traffic from the localhost to move directly to the Internet. Also, we can do port forwarding, and finally, we can have static nat to publish our DMZ server to the Internet.

In this scenario, we will practice "STATIC NAT " on the transport side.

Note: in some documents, this feature called "one to one" nat.

To achieve this goal, according to our topology, we need two essential steps.



I) on the Rome site, we need to have PAT for clients to reach the Internet.

II) on the Paris site, we need to have "STATIC NAT" for publishing our web server in DMZ to the public.

PART I

ROME SITE:

to achieve PAT in the Rome site, we need to configure PAT in vEdge Transport VPN, to understand the procedure you can follow this link:

https://www.networkingwithehsan.com/sd-wan-nat-part1

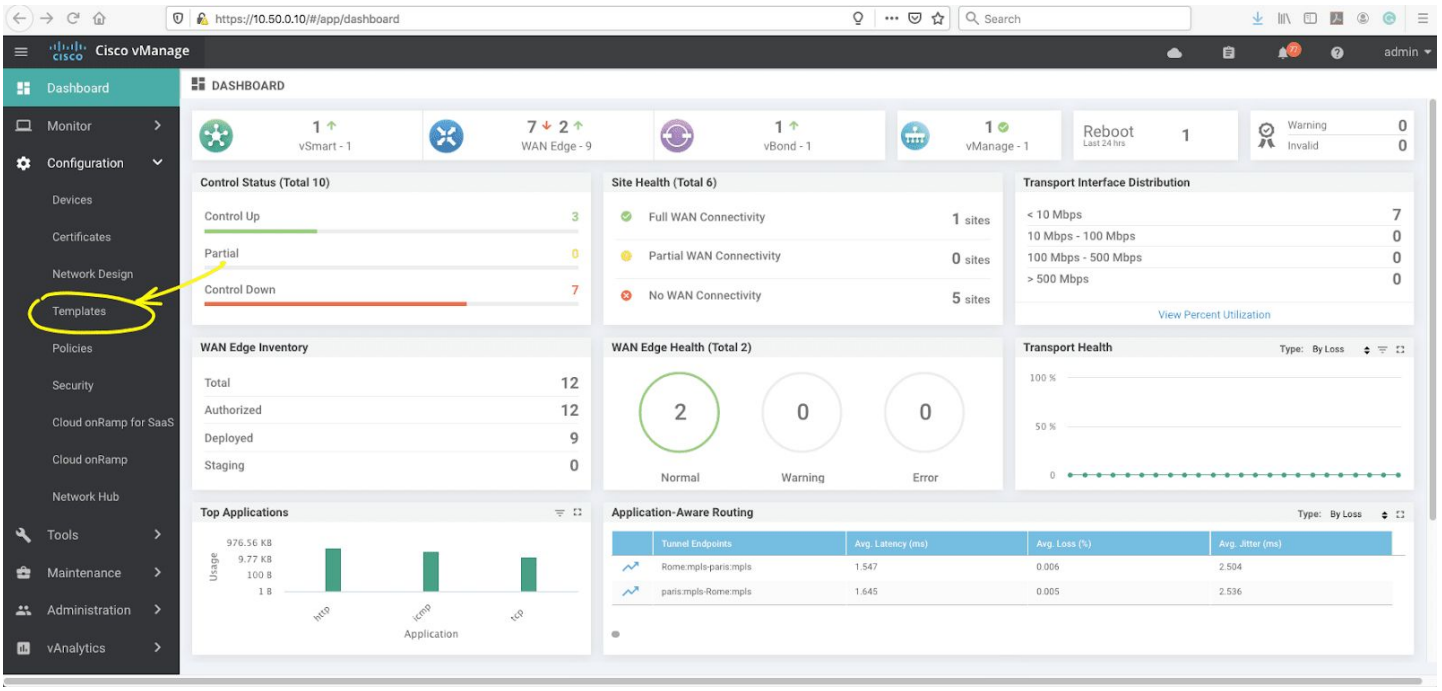
PART II

PARIS SITE:

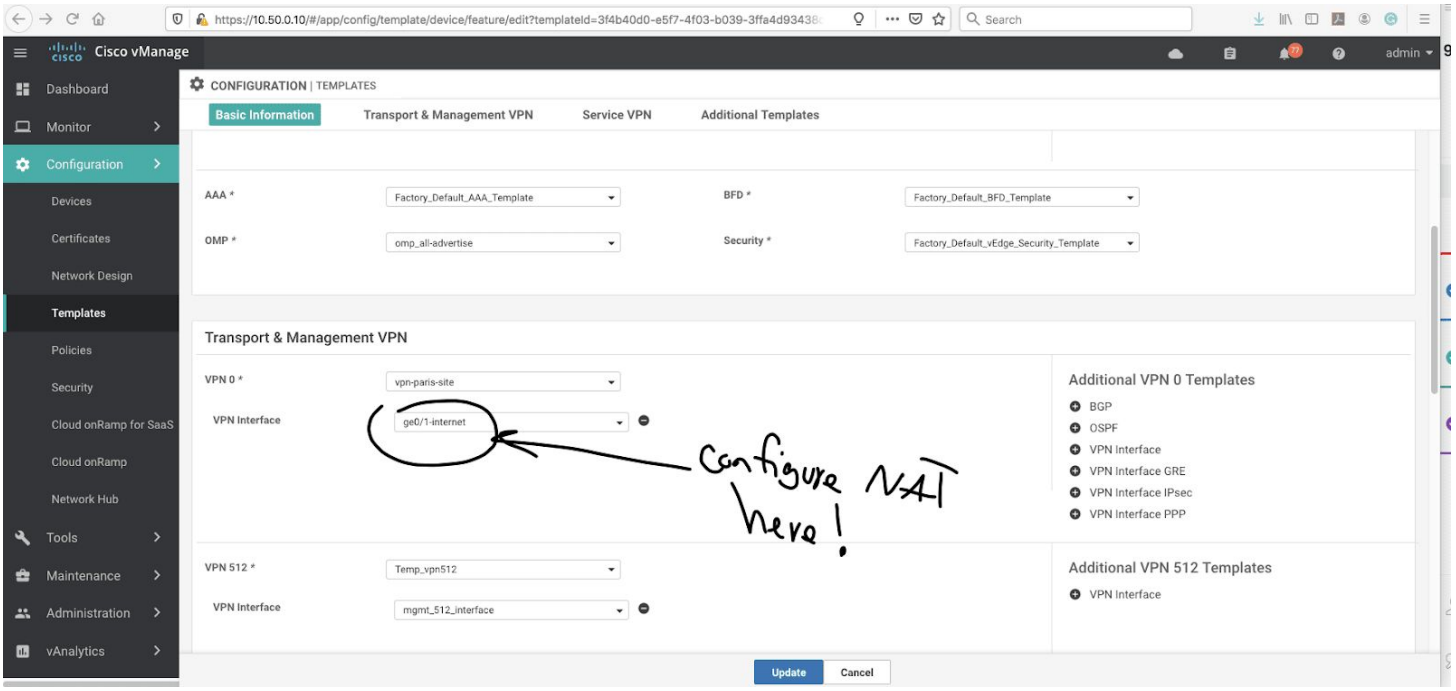
In my scenario, I am using vManage to do the configuration for Paris Site.

Step number one is to enable nat on the vedge router. (Transport VPN)

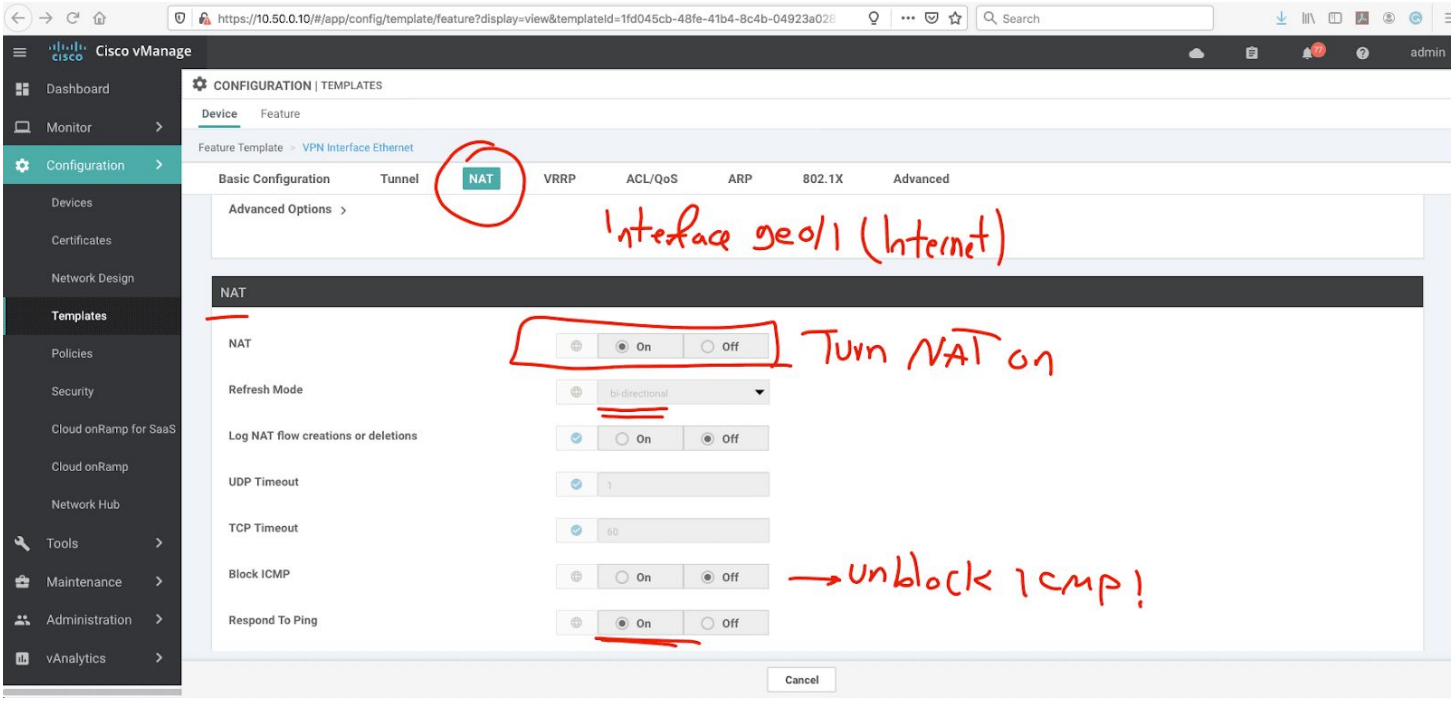
For this purpose, go to the "templates" menu and choose the Paris vedge profile.



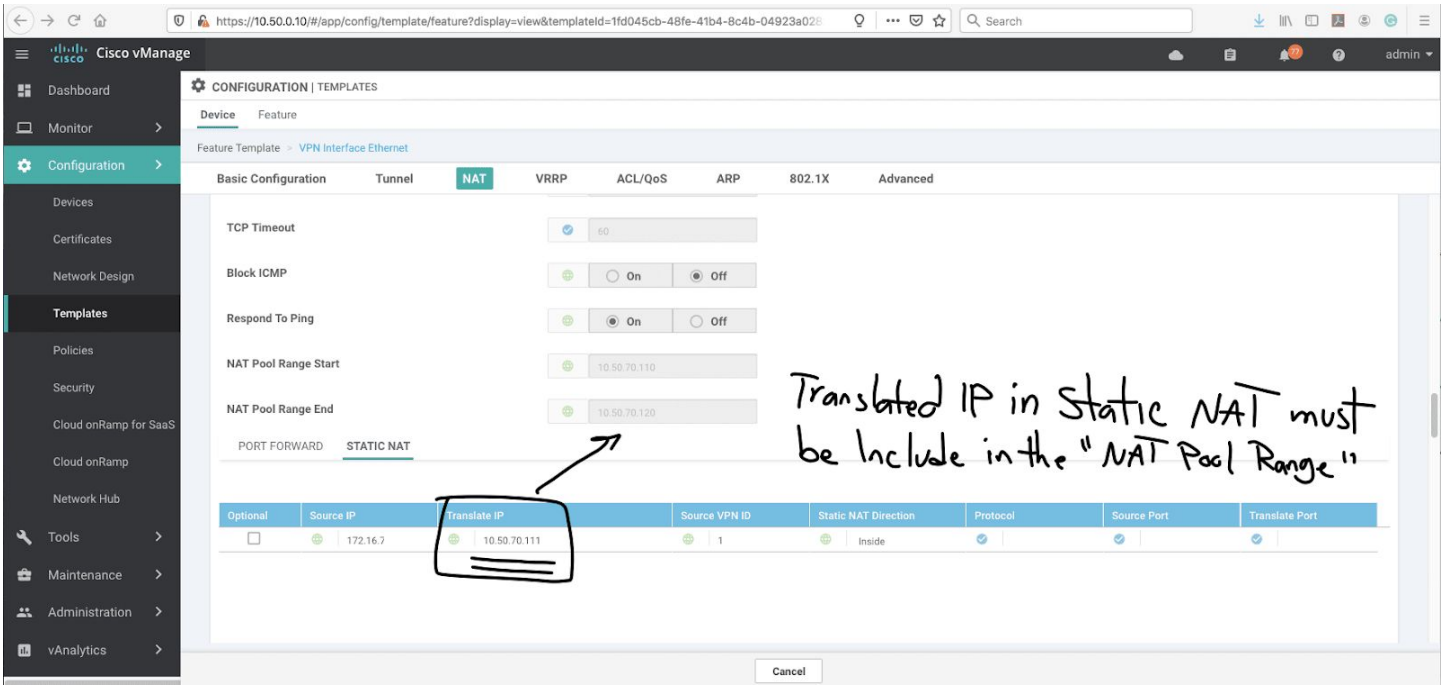
Then we have to select Interface under VPN 0 (Transport VPN)



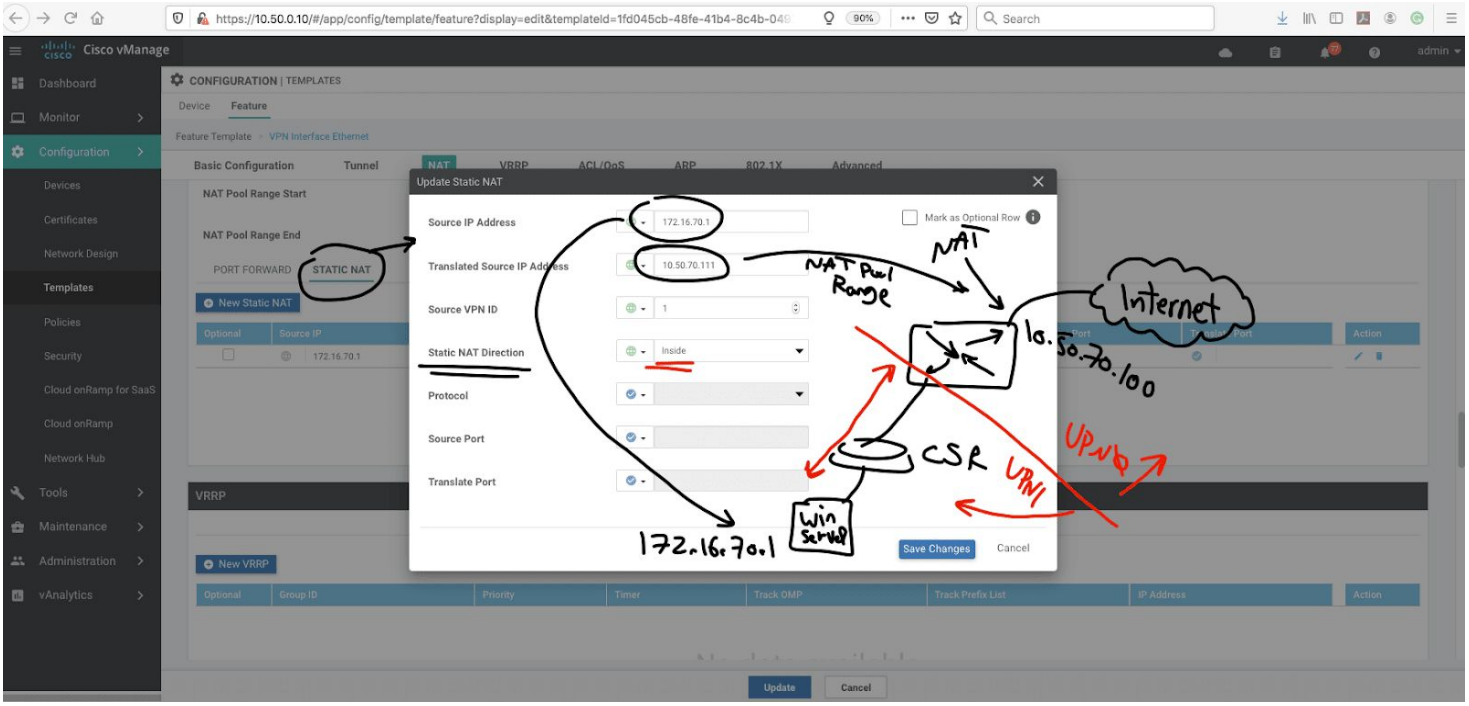
And enable the NAT in the profile.



Now, we have to create "NAT POOL RANGE."



After configuring the nat pool range, we need to choose "STATIC NAT" option and add static nat



That was the STATIC NAT config.

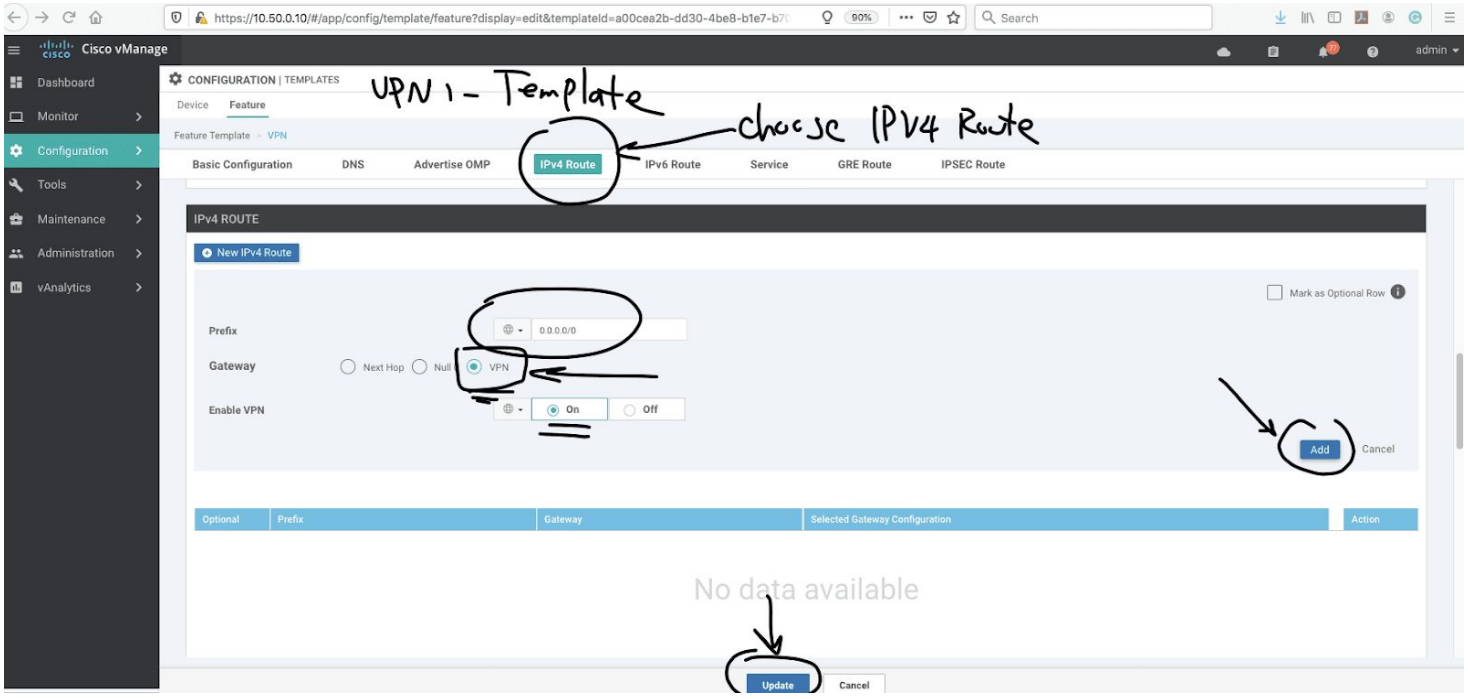
Let's make the final move.

In this action, we have to add a route in the service side (VPN 1) to VPN 0

Here is the procedure:

First, we go to VPN 1(in our scenario service VPN is VPN 1) template

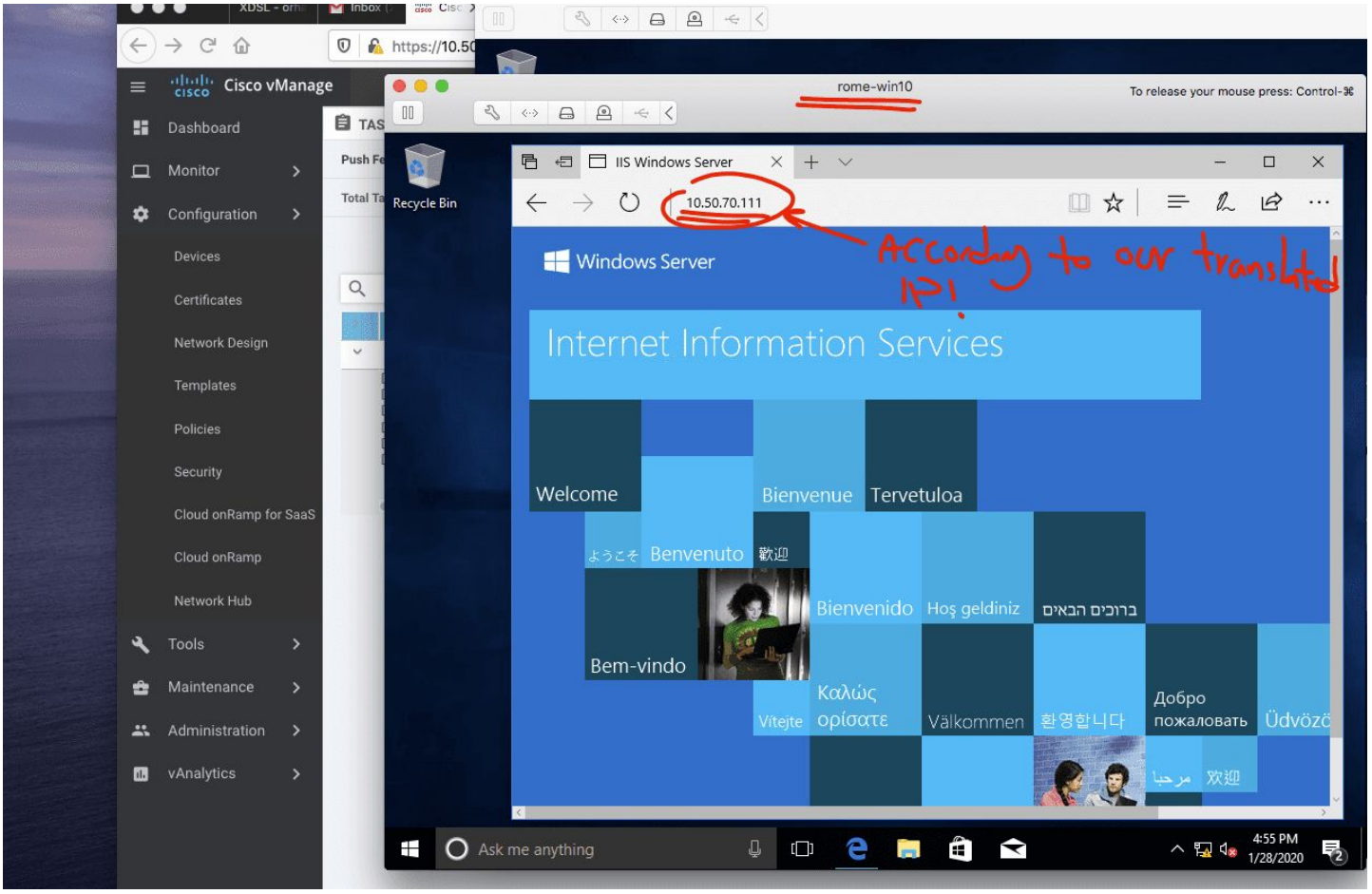
and add a default route to VPN 0



Note- remember to choose interested traffic for NAT.

Verification part:

Now we try to establish an HTTP connection from Rome client to Paris web server.

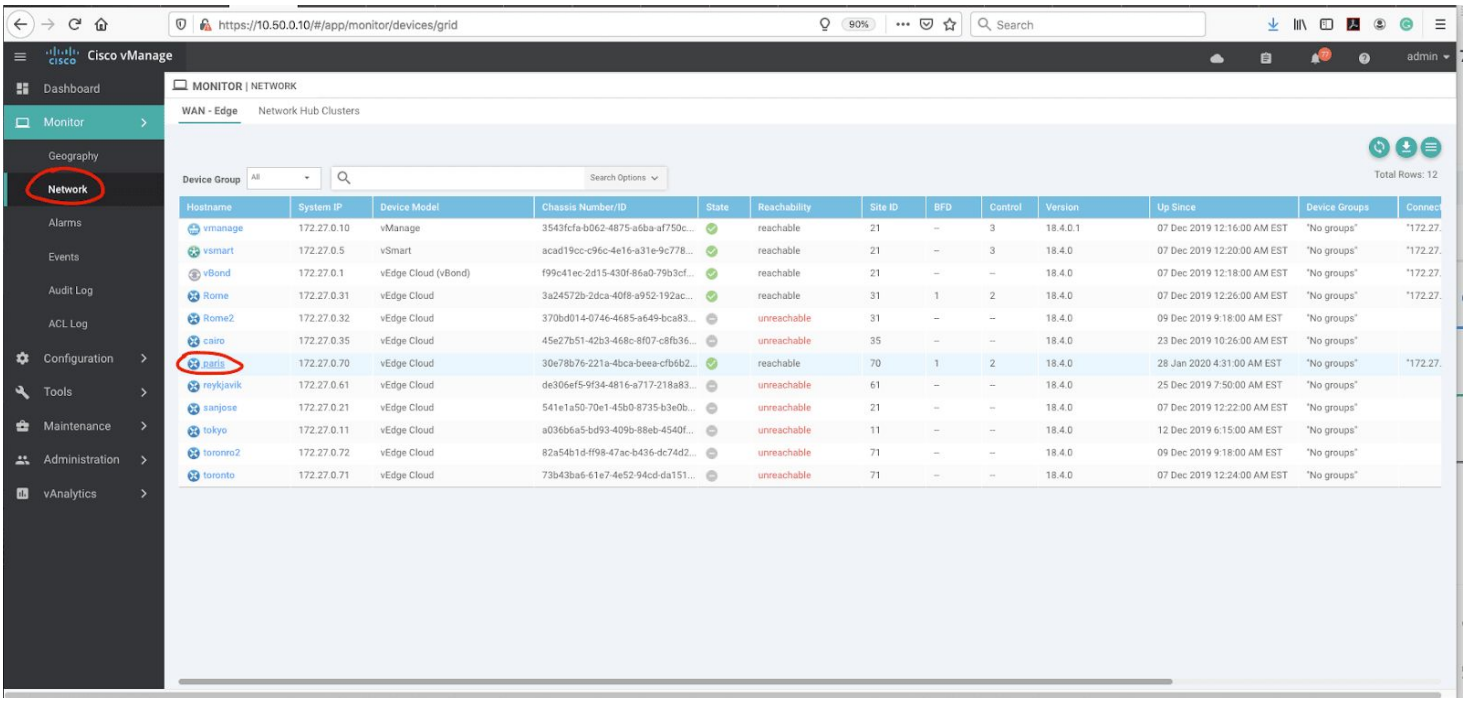


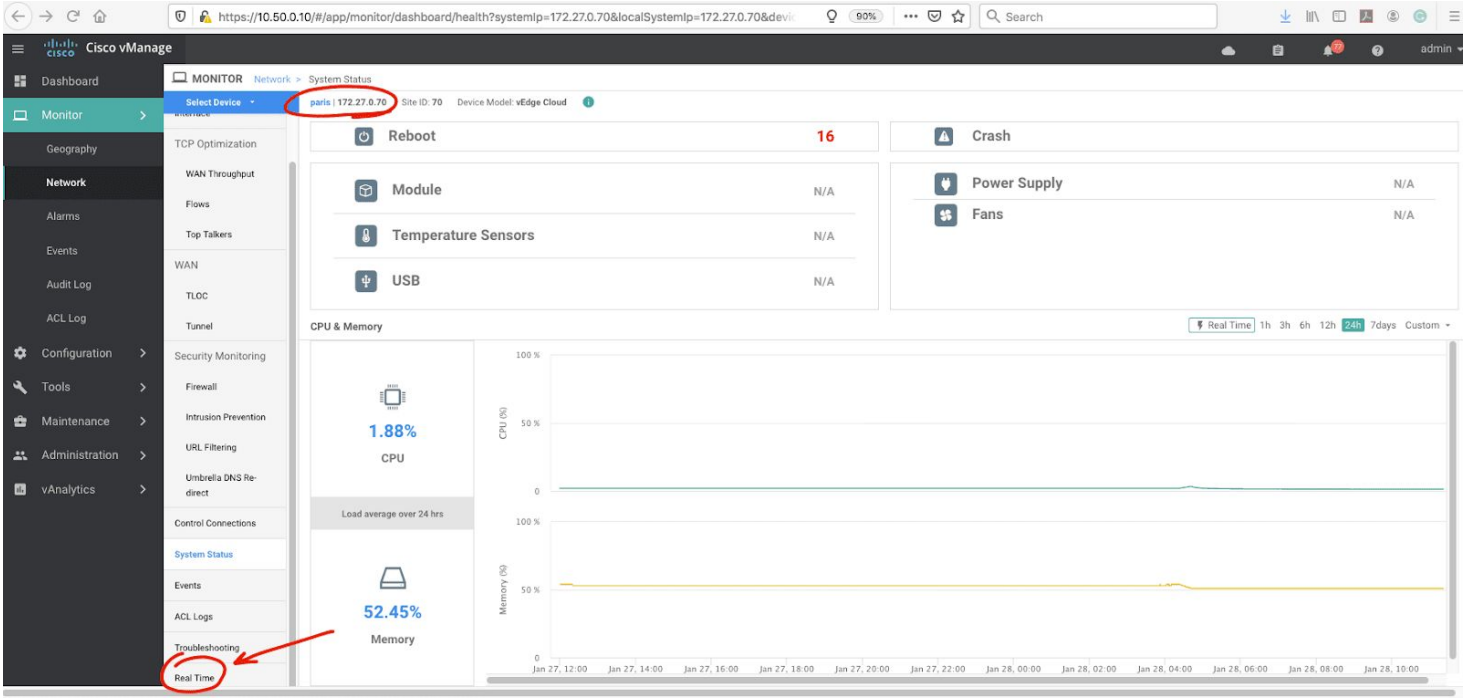
In Paris site, the public IP is 10.50.70.111(translated IP for web server)

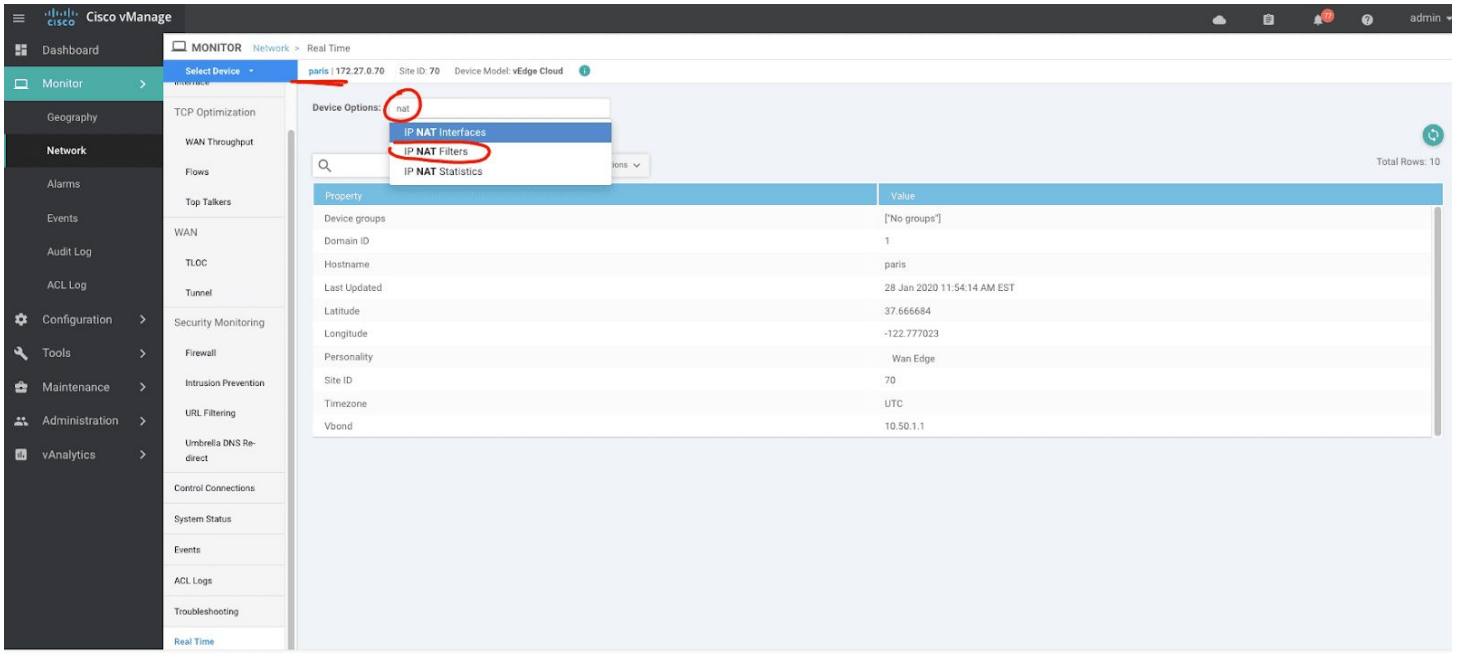
And I create static nat to "172.16.70.1," which is the Paris web server actual IP address.

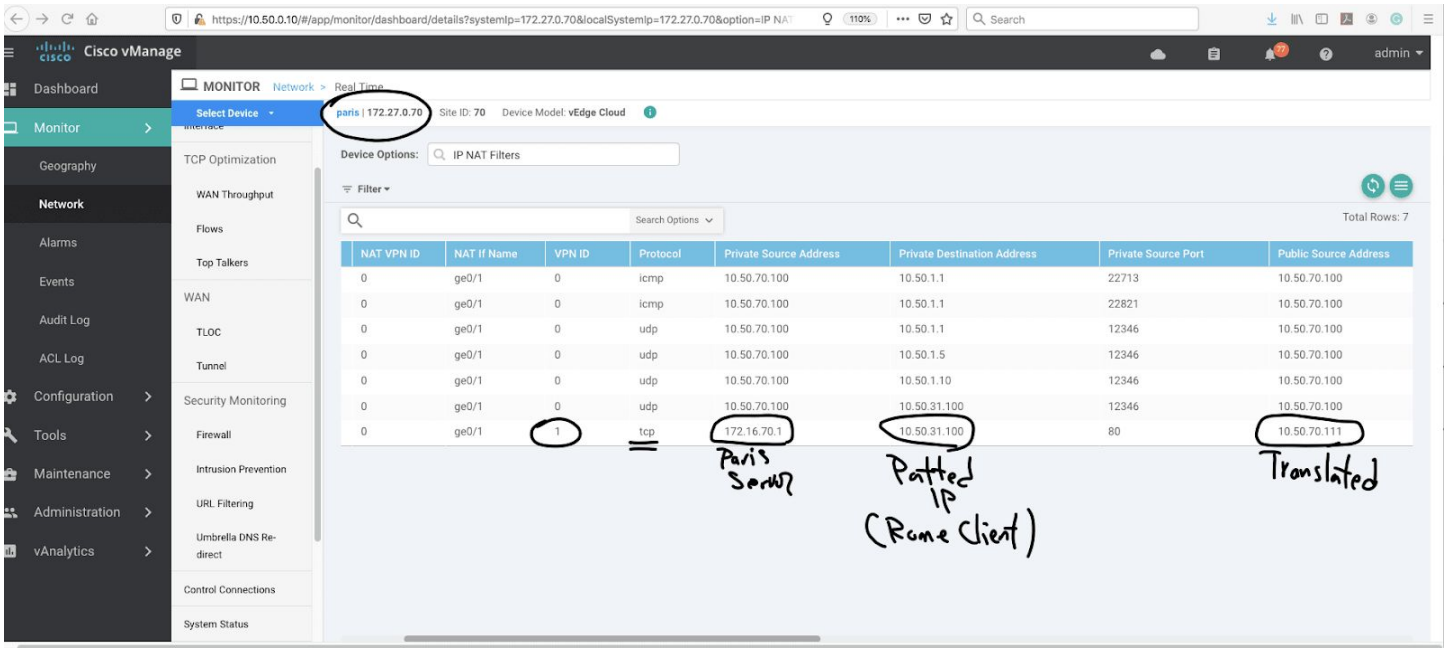
To understand more, I do the verification from vmanage.

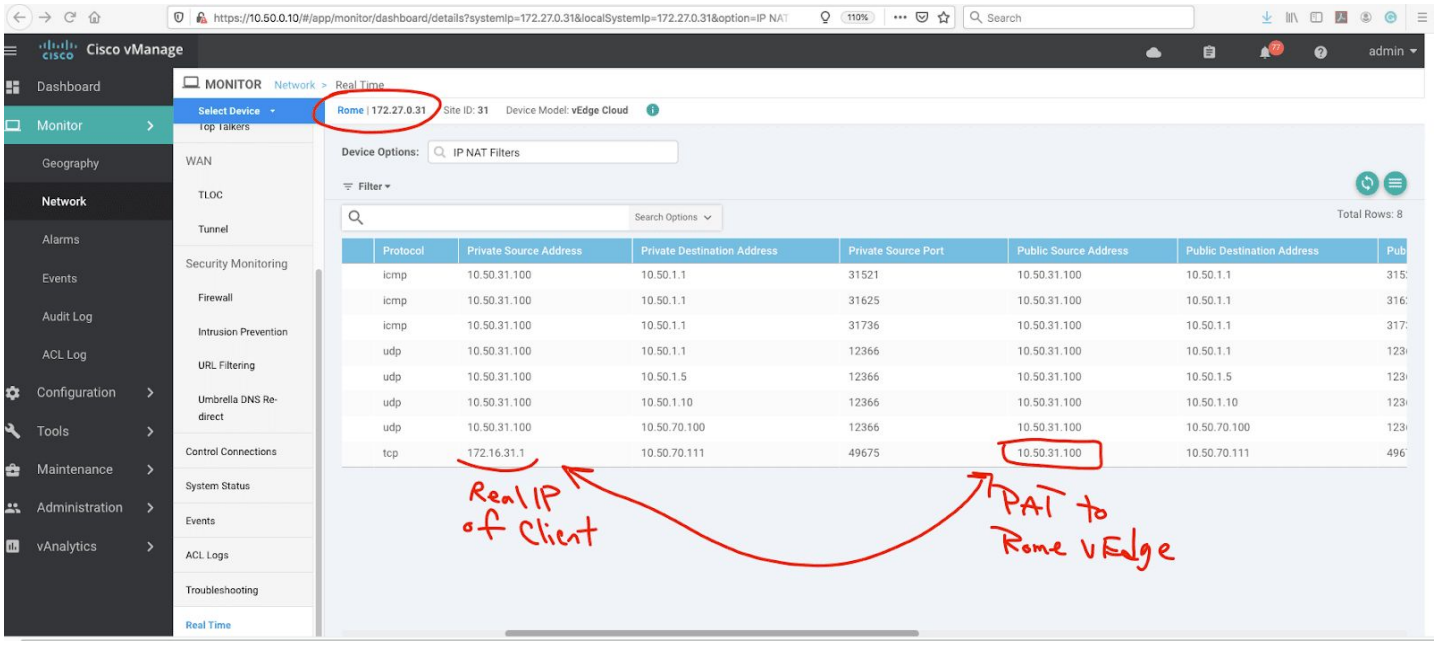
Let's check out






Cisco vManage
admin
Dashboard
Monitor
Geography
Network
Alarms
Events
Audit Log
ACL Log
Configuration
Tools
Maintenance
Administration
vAnalytics
MONITOR Network > Real Time
Select Device
paris | 172.27.0.70 Site ID: 70 Device Model: vEdge Cloud
TCP Optimization
WAN Throughput
Flows
Top Talkers
WAN
TLOC
Tunnel
Security Monitoring
Firewall
Intrusion Prevention
URL Filtering
Umbrella DNS Re-direct
Control Connections
System Status
Events
ACL Logs
Troubleshooting
Real Time
Device Options: nat
IP NAT Interfaces
IP NAT Filters
IP NAT Statistics
Total Rows: 10
Property
Value
Device groups
["No groups"]
Domain ID
1
Hostname
paris
Last Updated
28 Jan 2020 11:54:14 AM EST
Latitude
37.666684
Longitude
-122.777023
Personality
Wan Edge
Site ID
70
Timezone
UTC
Vbond
10.50.1.1


https://10.50.0.10/#/app/monitor/dashboard/details?systemIp=172.27.0.70&localSystemIp=172.27.0.70&option=IP NAT
Search
Cisco vManage
admin
Dashboard
Monitor
Geography
Network
Alarms
Events
Audit Log
ACL Log
Configuration
Tools
Maintenance
Administration
vAnalytics
MONITOR Network > Real Time
Select Device
paris | 172.27.0.70 Site ID: 70 Device Model: vEdge Cloud
TCP Optimization
WAN Throughput
Flows
Top Talkers
WAN
TLOC
Tunnel
Security Monitoring
Firewall
Intrusion Prevention
URL Filtering
Umbrella DNS Re-direct
Control Connections
System Status
Device Options: IP NAT Filters
Filter
Search Options
Total Rows: 7
NAT VPN ID
NAT If Name
VPN ID
Protocol
Private Source Address
Private Destination Address
Private Source Port
Public Source Address
0 ge0/1 0 icmp 10.50.70.100 10.50.1.1 22713 10.50.70.100
0 ge0/1 0 icmp 10.50.70.100 10.50.1.1 22821 10.50.70.100
0 ge0/1 0 udp 10.50.70.100 10.50.1.1 12346 10.50.70.100
0 ge0/1 0 udp 10.50.70.100 10.50.1.5 12346 10.50.70.100
0 ge0/1 0 udp 10.50.70.100 10.50.1.10 12346 10.50.70.100
0 ge0/1 0 udp 10.50.70.100 10.50.31.100 12346 10.50.70.100
0 ge0/1 1 tcp 172.16.70.1 10.50.31.100 80 10.50.70.111
Paris Server
Patted IP (Rome Client)
Translated



So as you can see the client in Rome is patted to Rome vEdge Public address and try to reach Paris translated IP address (Public Address of web server).

The Paris vEdge do the STATIC NAT and web server in DMZ is reachable for Rome Client.

Thank you for viewing