

# Cisco SD-WAN - Static NAT (PART III)

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

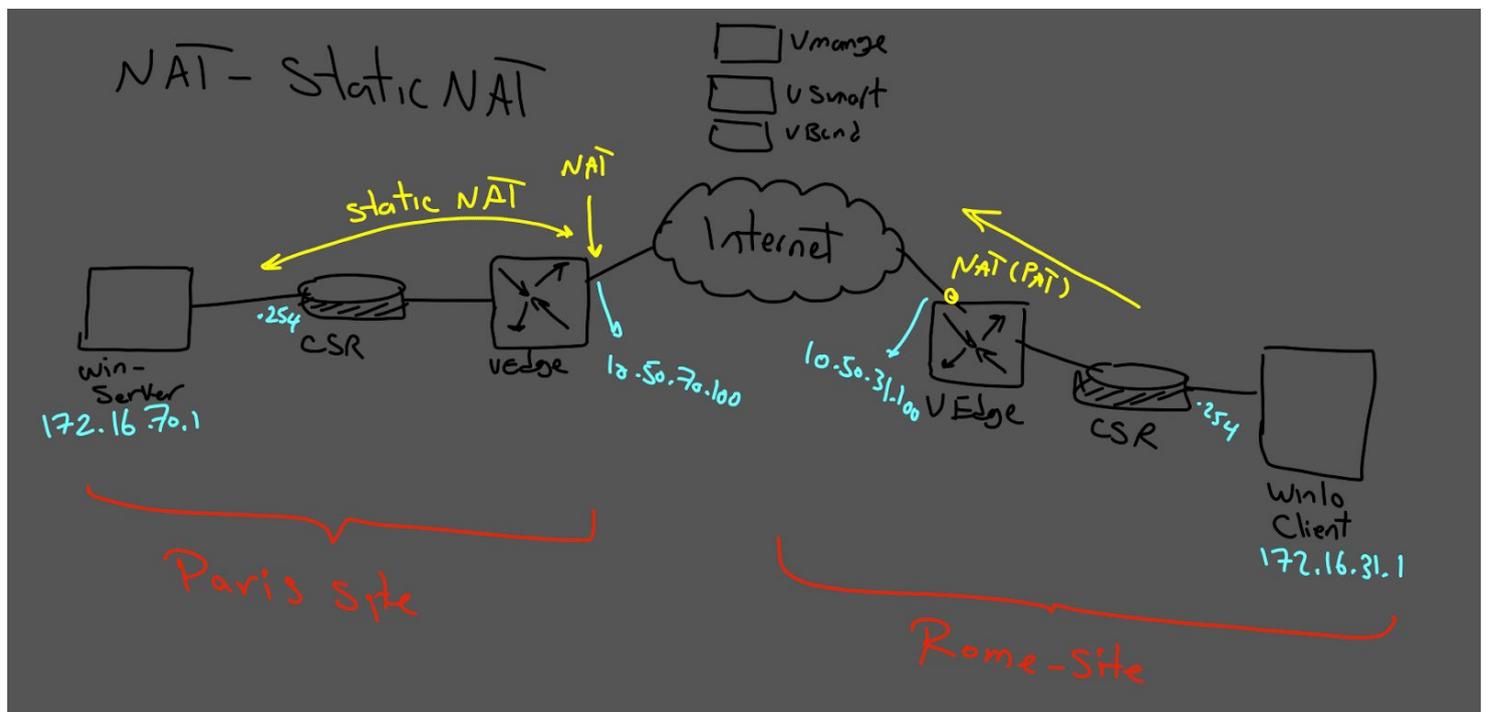
A vEdge cloud router can play a NAT role. It can do the natting both on the transport side ( VPN 0 ) and on the service side ( VPN 1, for example).

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.networkingwithhsan.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)

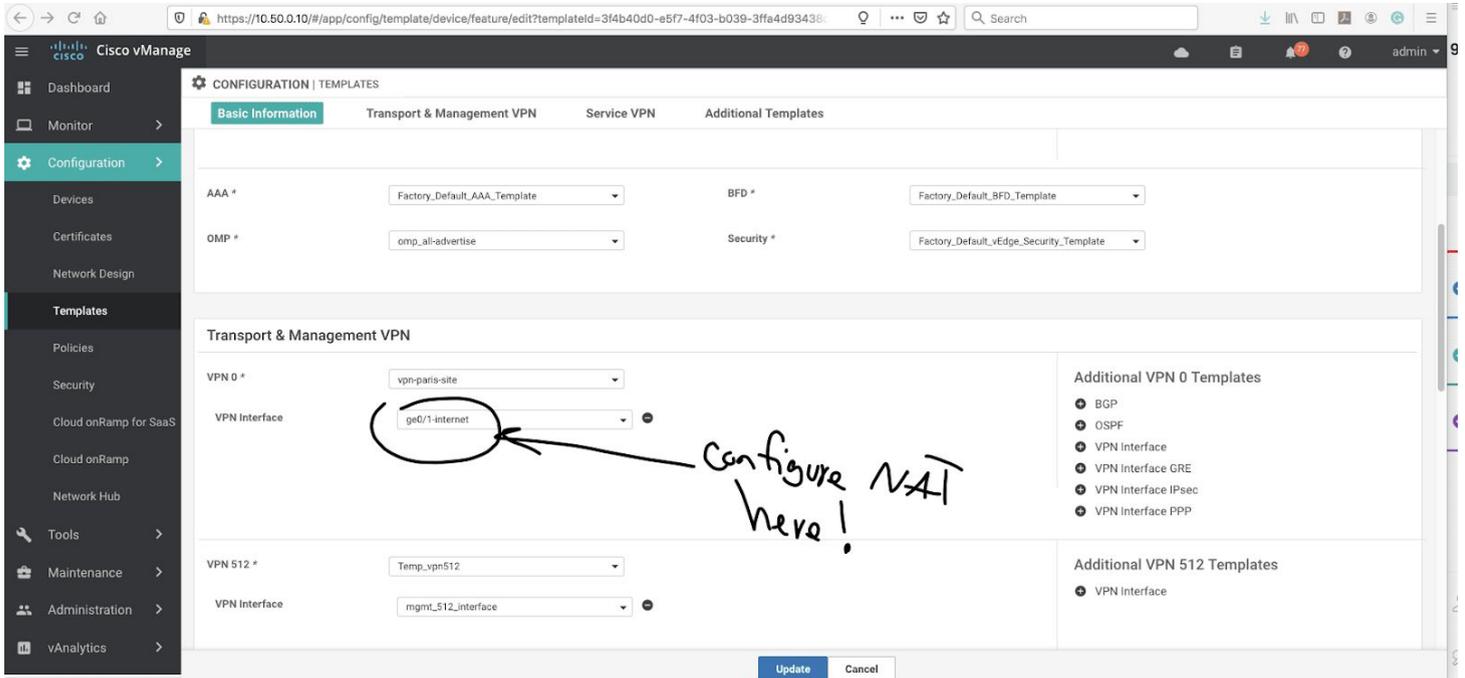
For this purpose, go to the "templates" menu and choose the Paris vedge profile.

The screenshot displays the Cisco vManage dashboard interface. The left sidebar contains a navigation menu with the following items: Dashboard, Monitor, Configuration, Devices, Certificates, Network Design, Templates (highlighted with a yellow circle), Policies, Security, Cloud onRamp for SaaS, Cloud onRamp, Network Hub, Tools, Maintenance, Administration, and vAnalytics. The main dashboard area shows several key performance indicators (KPIs) and charts:

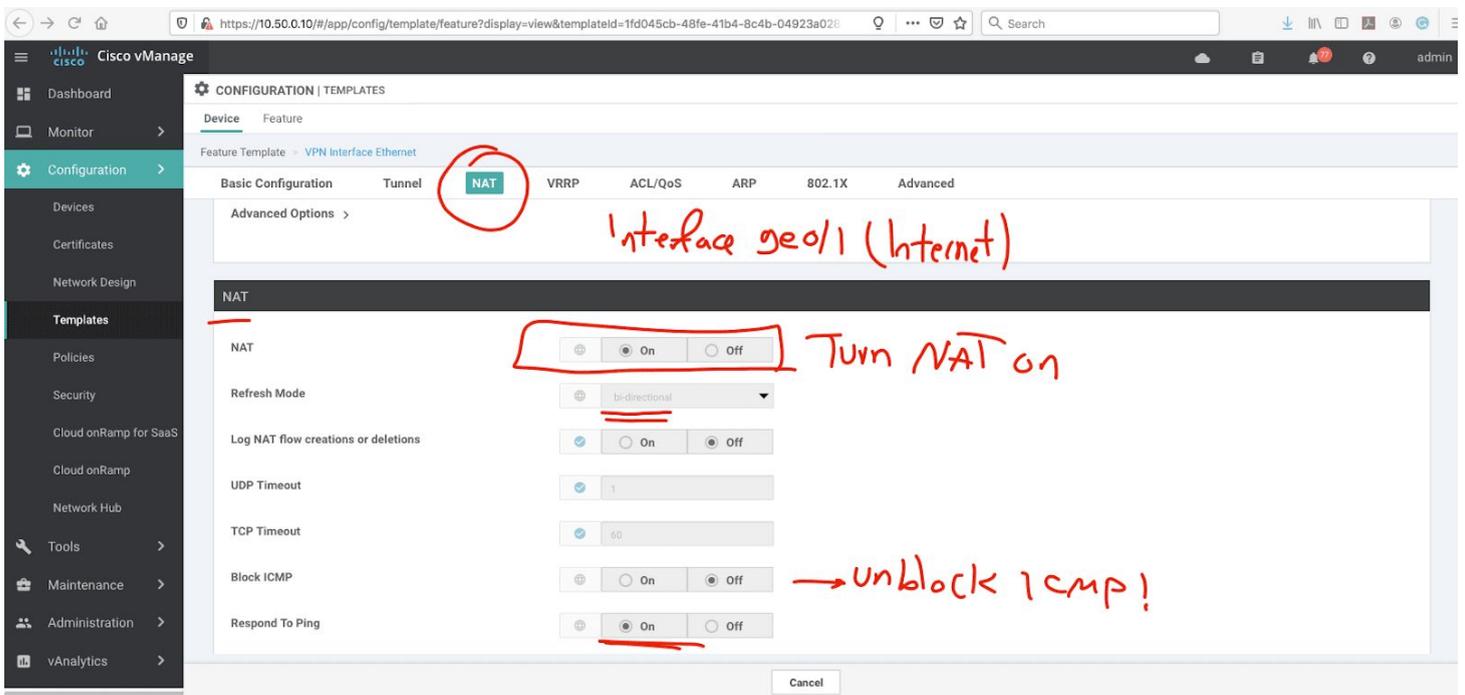
- Control Status (Total 10):** A progress bar chart showing 3 Control Up, 0 Partial, and 7 Control Down.
- Site Health (Total 6):** A summary of WAN connectivity: 1 site with Full WAN Connectivity, 0 sites with Partial WAN Connectivity, and 5 sites with No WAN Connectivity.
- Transport Interface Distribution:** A bar chart showing bandwidth utilization: 7 sites < 10 Mbps, 0 sites 10 Mbps - 100 Mbps, 0 sites 100 Mbps - 500 Mbps, and 0 sites > 500 Mbps.
- WAN Edge Inventory:** A table showing 12 Total, 12 Authorized, 9 Deployed, and 0 Staging.
- WAN Edge Health (Total 2):** Three circular gauges showing 2 Normal, 0 Warning, and 0 Error.
- Transport Health:** A line graph showing 100% health.
- Top Applications:** A bar chart showing usage for http, https, and ftp.
- Application-Aware Routing:** A table showing tunnel endpoints, average latency, average loss, and average jitter.

Tunnel Endpoints	Avg. Latency (ms)	Avg. Loss (%)	Avg. Jitter (ms)
Rome:mpls-paris:mpls	1.547	0.006	2.504
paris:mpls-Rome:mpls	1.645	0.005	2.536

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."

Translated IP in Static NAT must be include in the "NAT Pool Range"

Optional	Source IP	Translate IP	Source VPN ID	Static NAT Direction	Protocol	Source Port	Translate Port
<input type="checkbox"/>	172.16.7	10.50.70.111	1	Inside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

Internet

CSR VPN

UP/DN

Win Server

172.16.70.1

10.50.70.111

NAT Pool Range

NAT

That was the STATIC NAT config.

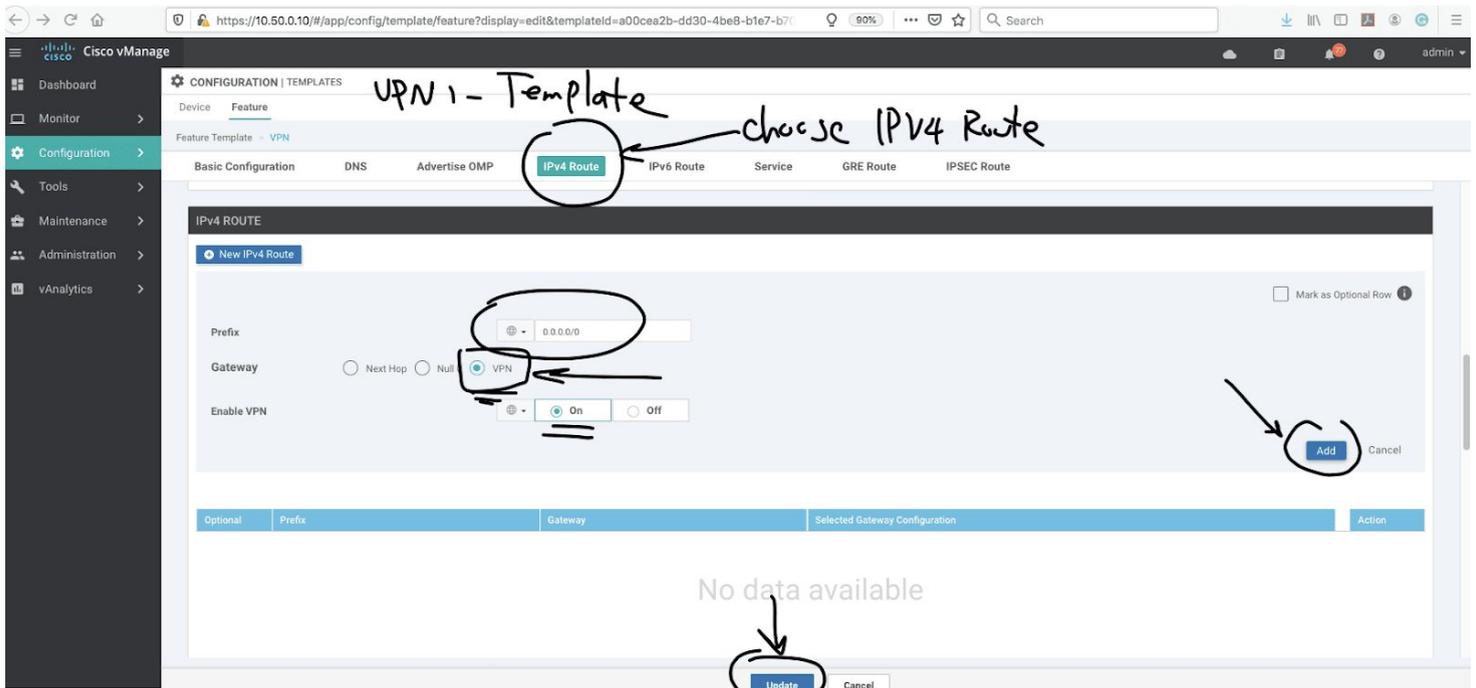
Let's make the final move.

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

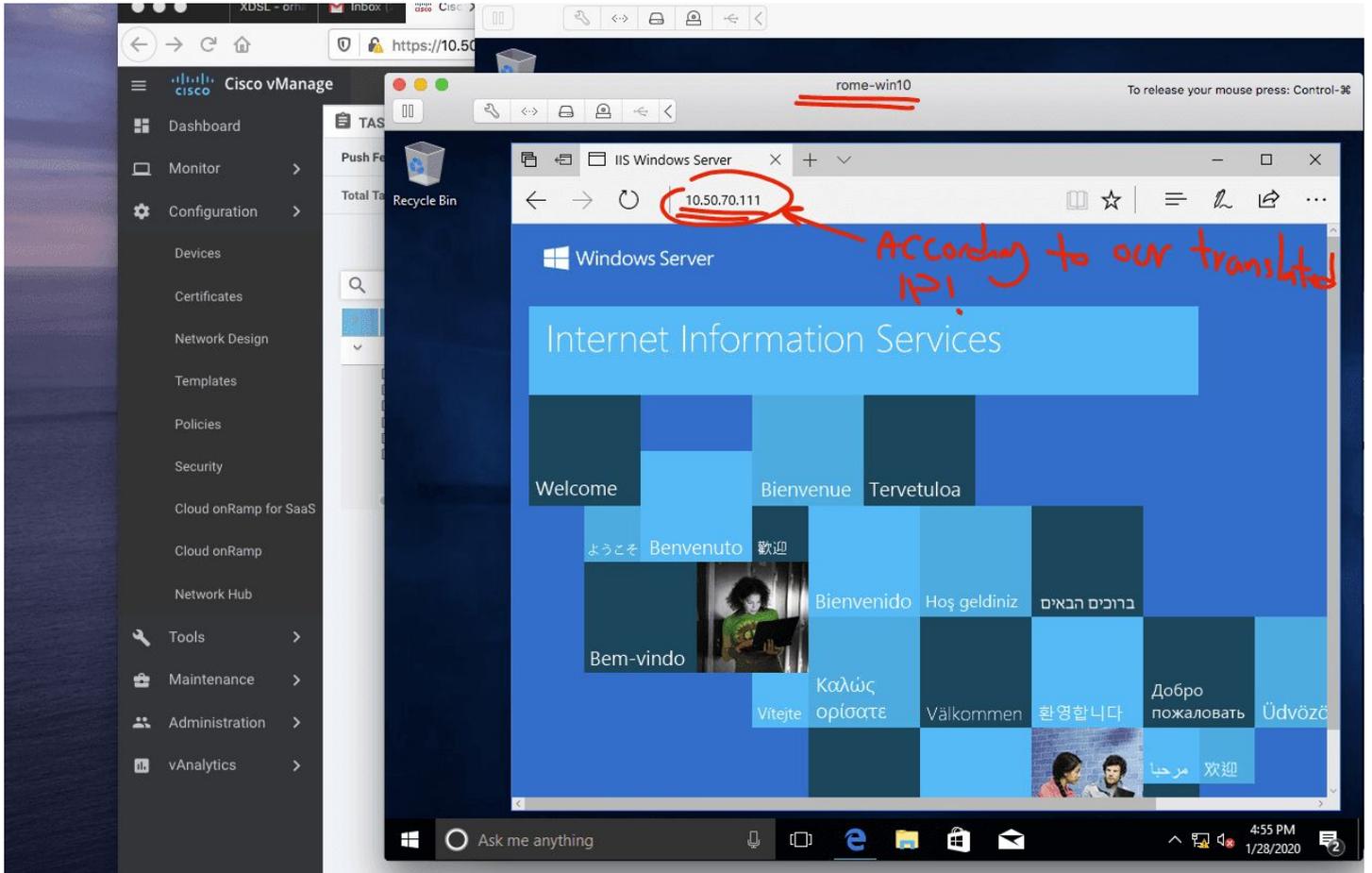
and add a default route to VPN 0



**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)

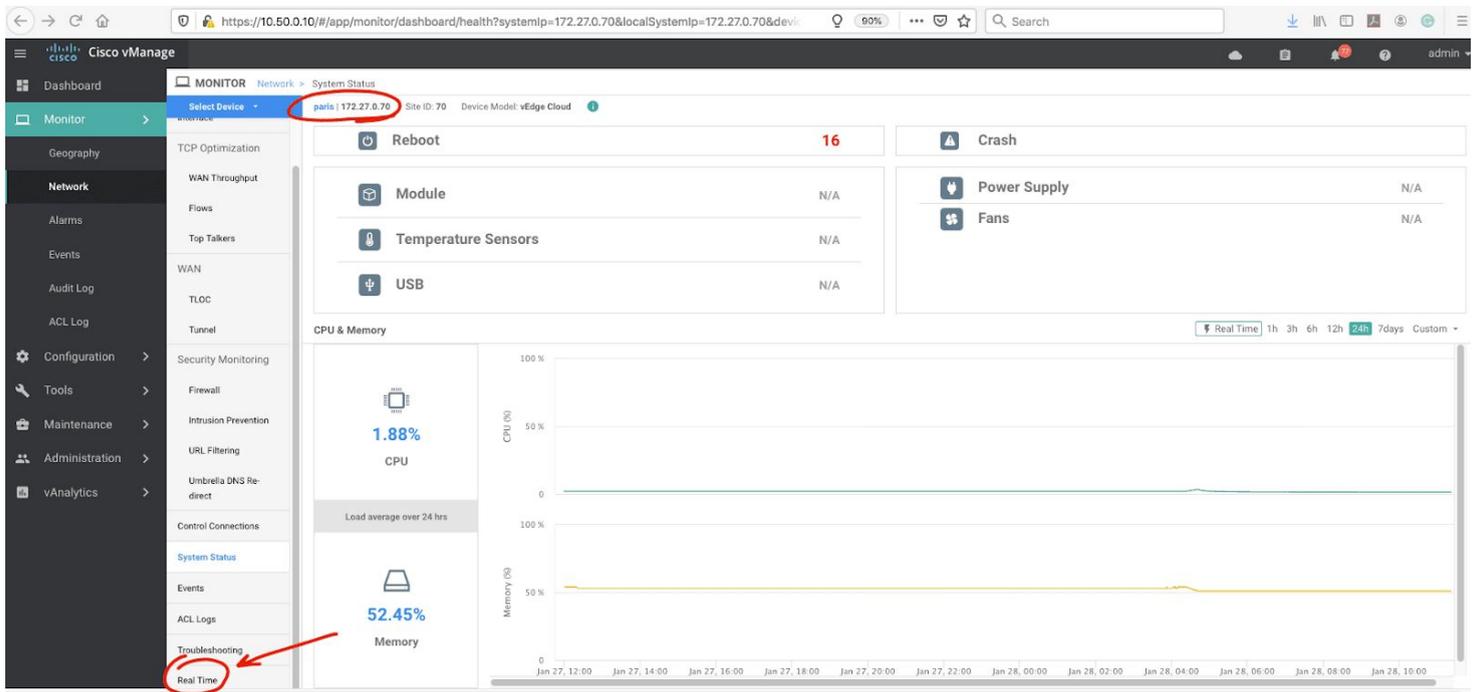
And I create static nat to "172.16.70.1," which is the Paris web server actual IP address.

To understand more, I do the verification from vmanage.

Let's check out

The screenshot shows the Cisco vManage interface for monitoring network devices. The 'Network' menu item in the left sidebar is circled in red. The main content area displays a table of devices under the 'WAN - Edge' section. The 'paris' device is highlighted with a red circle in the table.

Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control	Version	Up Since	Device Groups	Connect
vmanage	172.27.0.10	vManage	3543cfab062-4875-a6ba-af750c...	✓	reachable	21	-	3	18.4.0.1	07 Dec 2019 12:16:00 AM EST	"No groups"	"172.27.
vsmart	172.27.0.5	vSmart	acad19cc-c96c-4e16-a31e-9c778...	✓	reachable	21	-	3	18.4.0	07 Dec 2019 12:20:00 AM EST	"No groups"	"172.27.
vBond	172.27.0.1	vEdge Cloud (vBond)	f99c41ec-2d15-430f-86a0-79b3cf...	✓	reachable	21	-	-	18.4.0	07 Dec 2019 12:18:00 AM EST	"No groups"	"172.27.
Rome	172.27.0.31	vEdge Cloud	3a24572b-2dca-40f8-a952-192ac...	✓	reachable	31	1	2	18.4.0	07 Dec 2019 12:26:00 AM EST	"No groups"	"172.27.
Rome2	172.27.0.32	vEdge Cloud	370bd014-0746-4685-a649-bca83...	✗	unreachable	31	-	-	18.4.0	09 Dec 2019 9:18:00 AM EST	"No groups"	
cairo	172.27.0.35	vEdge Cloud	45e27b51-42b3-468c-8f07-c8fb36...	✗	unreachable	35	-	-	18.4.0	23 Dec 2019 10:26:00 AM EST	"No groups"	
paris	172.27.0.70	vEdge Cloud	30e78b76-221a-4bca-beea-cfb6b2...	✓	reachable	70	1	2	18.4.0	28 Jan 2020 4:31:00 AM EST	"No groups"	"172.27.
reykjavik	172.27.0.61	vEdge Cloud	de305ef5-9f34-4816-a717-218a83...	✗	unreachable	61	-	-	18.4.0	25 Dec 2019 7:50:00 AM EST	"No groups"	
sanjose	172.27.0.21	vEdge Cloud	541e1a50-70e1-45b0-8735-b3e0b...	✗	unreachable	21	-	-	18.4.0	07 Dec 2019 12:22:00 AM EST	"No groups"	
tokyo	172.27.0.11	vEdge Cloud	a036b6a5-bd93-409b-88eb-4540f...	✗	unreachable	11	-	-	18.4.0	12 Dec 2019 6:15:00 AM EST	"No groups"	
toronto2	172.27.0.72	vEdge Cloud	82a54b1d-f998-47ac-b436-dc74d2...	✗	unreachable	71	-	-	18.4.0	09 Dec 2019 9:18:00 AM EST	"No groups"	
toronto	172.27.0.71	vEdge Cloud	73b43ba6-61e7-4e52-94cd-d1a151...	✗	unreachable	71	-	-	18.4.0	07 Dec 2019 12:24:00 AM EST	"No groups"	



Cisco vManage MONITOR Network > Real Time

Select Device: paris | 172.27.0.70 Site ID: 70 Device Model: vEdge Cloud

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

Cisco vManage MONITOR Network > Real Time

Select Device: paris | 172.27.0.70 Site ID: 70 Device Model: vEdge Cloud

Device Options: IP NAT Filters

Filter

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 (Same Client) Translated

MONITOR Network > Real Time

Select Device: Rome | 172.27.0.31 Site ID: 31 Device Model: vEdge Cloud

Device Options: IP NAT Filters

Protocol	Private Source Address	Private Destination Address	Private Source Port	Public Source Address	Public Destination Address	Pub
icmp	10.50.31.100	10.50.1.1	31521	10.50.31.100	10.50.1.1	315
icmp	10.50.31.100	10.50.1.1	31625	10.50.31.100	10.50.1.1	316
icmp	10.50.31.100	10.50.1.1	31736	10.50.31.100	10.50.1.1	317
udp	10.50.31.100	10.50.1.1	12366	10.50.31.100	10.50.1.1	123
udp	10.50.31.100	10.50.1.5	12366	10.50.31.100	10.50.1.5	123
udp	10.50.31.100	10.50.1.10	12366	10.50.31.100	10.50.1.10	123
udp	10.50.31.100	10.50.70.100	12366	10.50.31.100	10.50.70.100	123
tcp	172.16.31.1	10.50.70.111	49675	10.50.31.100	10.50.70.111	496

Handwritten annotations: "Real IP of Client" points to 172.16.31.1; "PAT to Rome vEdge" points to 10.50.31.100.

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