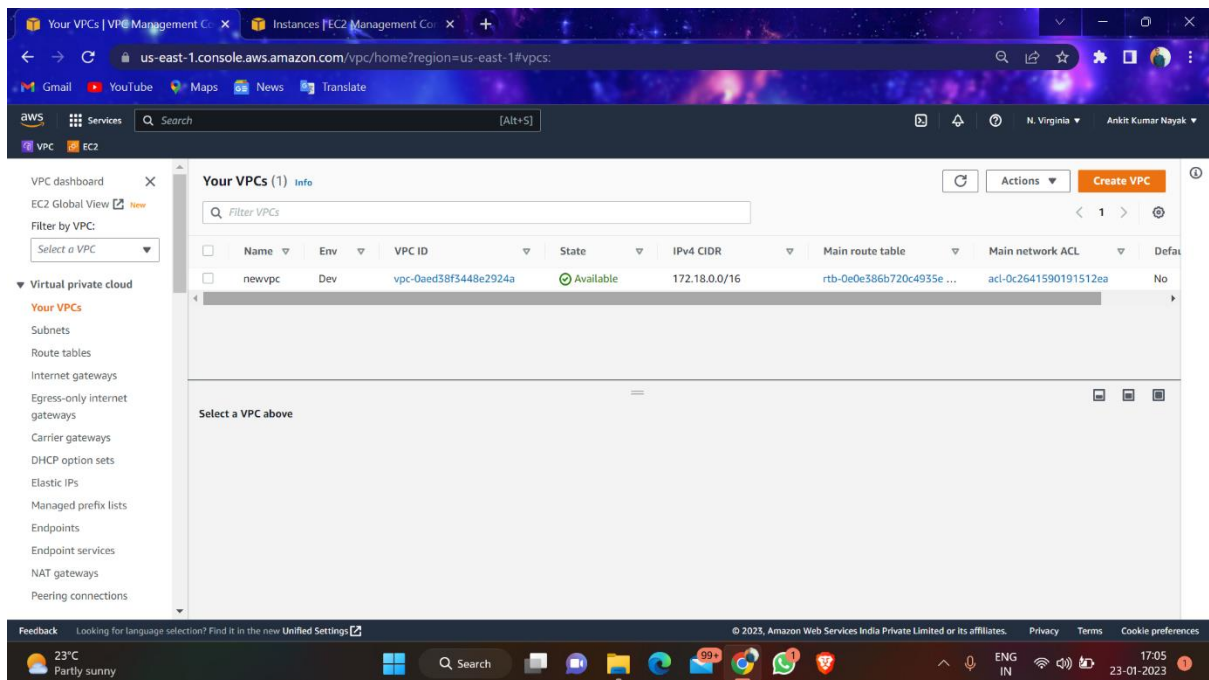
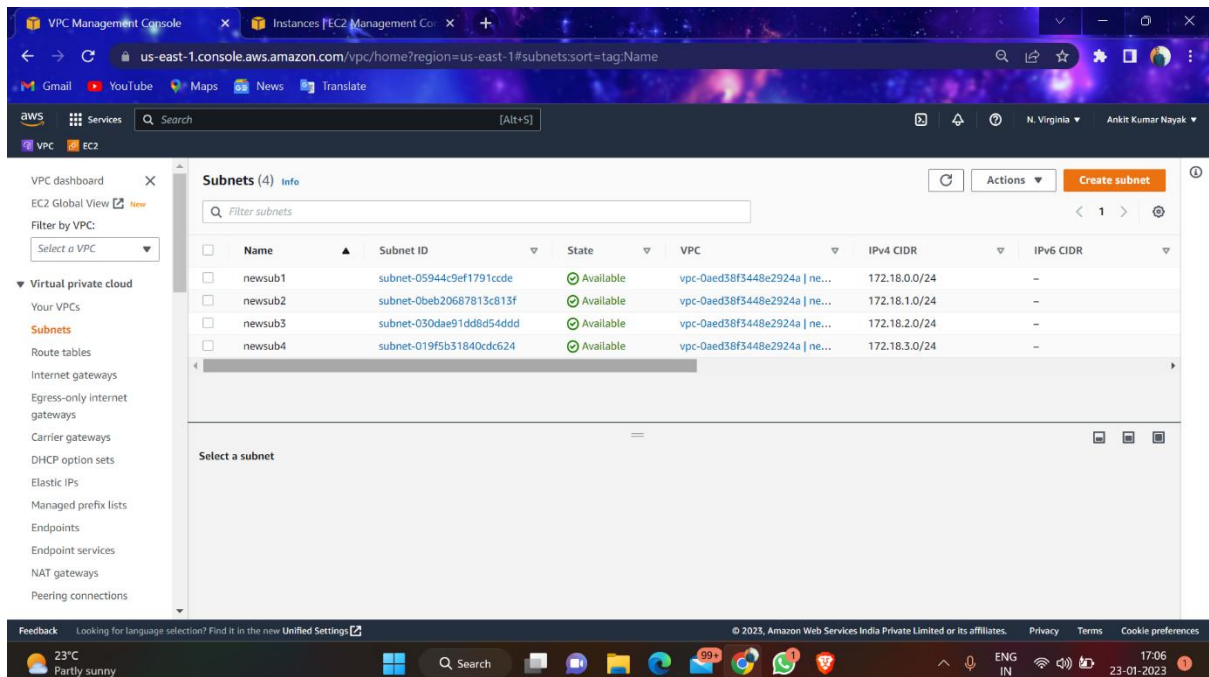


Establishing a NAT Instance

1-Creating VPC



2-Creating Subnet



3-Assigning Subnet Association

The screenshot shows the AWS VPC Management Console interface. The breadcrumb trail is: VPC > Route tables > rtb-0403421ab5eef76dd > Edit subnet associations. The page title is 'Edit subnet associations' with a subtitle 'Change which subnets are associated with this route table.' Below this, there is a section 'Available subnets (2/4)' with a search bar and a table of subnets. Two subnets are selected: 'newsub3' and 'newsub4'. Below the table, there is a 'Selected subnets' section showing the selected subnets as tags: 'subnet-030dae91dd8d54ddd / newsub3' and 'subnet-019f5b31840cdc624 / newsub4'. At the bottom right, there are 'Cancel' and 'Save associations' buttons.

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	newsub3	subnet-030dae91dd8d54ddd	172.18.2.0/24	-	rtb-0403421ab5eef76dd / newroute
<input type="checkbox"/>	newsub1	subnet-05944c9ef1791ccde	172.18.0.0/24	-	Main (rtb-0e0e386b720c4935e / Default)
<input checked="" type="checkbox"/>	newsub4	subnet-019f5b31840cdc624	172.18.3.0/24	-	rtb-0403421ab5eef76dd / newroute
<input type="checkbox"/>	newsub2	subnet-0beb20687813c813f	172.18.1.0/24	-	Main (rtb-0e0e386b720c4935e / Default)

Selected subnets

subnet-030dae91dd8d54ddd / newsub3 subnet-019f5b31840cdc624 / newsub4

4-Creating Route Table

The screenshot shows the AWS VPC Management Console interface. The breadcrumb trail is: VPC > Route tables > Route tables (2). The page title is 'Route tables (2)' with a subtitle 'Info'. Below this, there is a search bar and a table of route tables. Two route tables are listed: 'Default' and 'newroute'. At the bottom right, there is a 'Create route table' button.

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
<input type="checkbox"/>	Default	rtb-0e0e386b720c4935e	-	-	Yes	vpc-0aed38f3448e2924a ne...	5370244433...
<input type="checkbox"/>	newroute	rtb-0403421ab5eef76dd	2 subnets	-	No	vpc-0aed38f3448e2924a ne...	5370244433...

Select a route table

5-Inside Default Route Table

VPC Management Console

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes:RouteTableId=rtb-0e0e386b720c4935e

VPC > Route tables > rtb-0e0e386b720c4935e > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.18.0.0/16	local	Active	No
0.0.0.0/0	igw-0afdc02212fdd799	Active	No

Buttons: Add route, Cancel, Preview, Save changes

6-Inside New Route Table

VPC Management Console

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#EditRoutes:RouteTableId=rtb-0403421ab5eef76dd

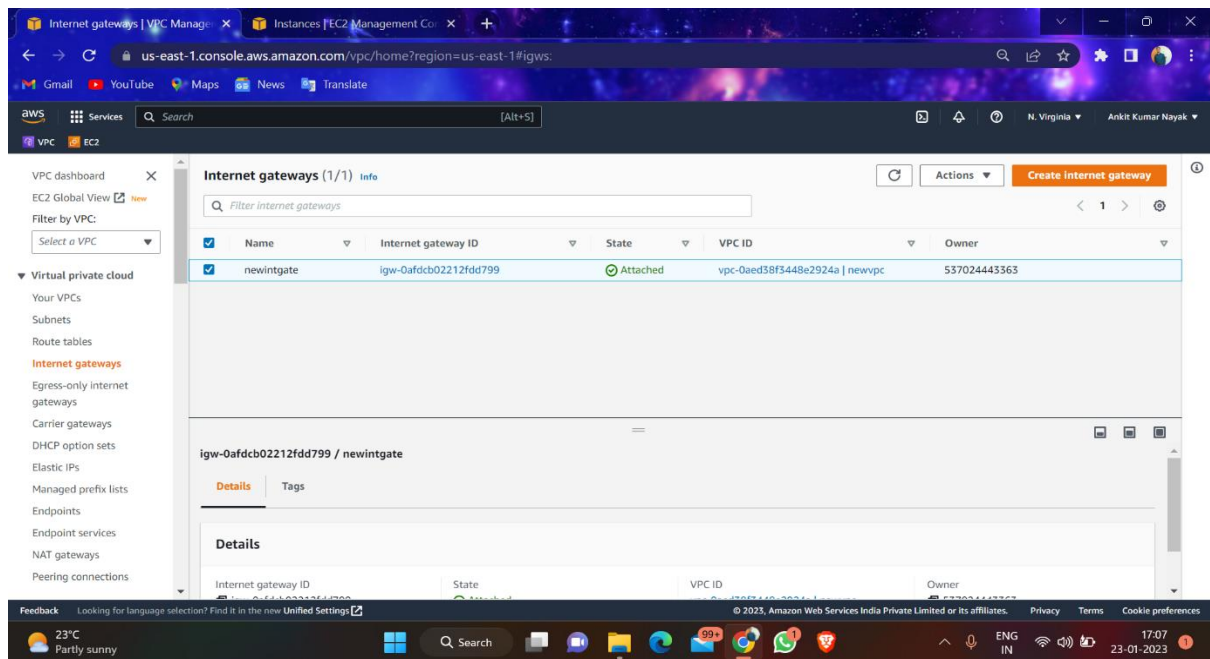
VPC > Route tables > rtb-0403421ab5eef76dd > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.18.0.0/16	local	Active	No
0.0.0.0/0	eni-07664b9bd03f4ecc3	Active	No

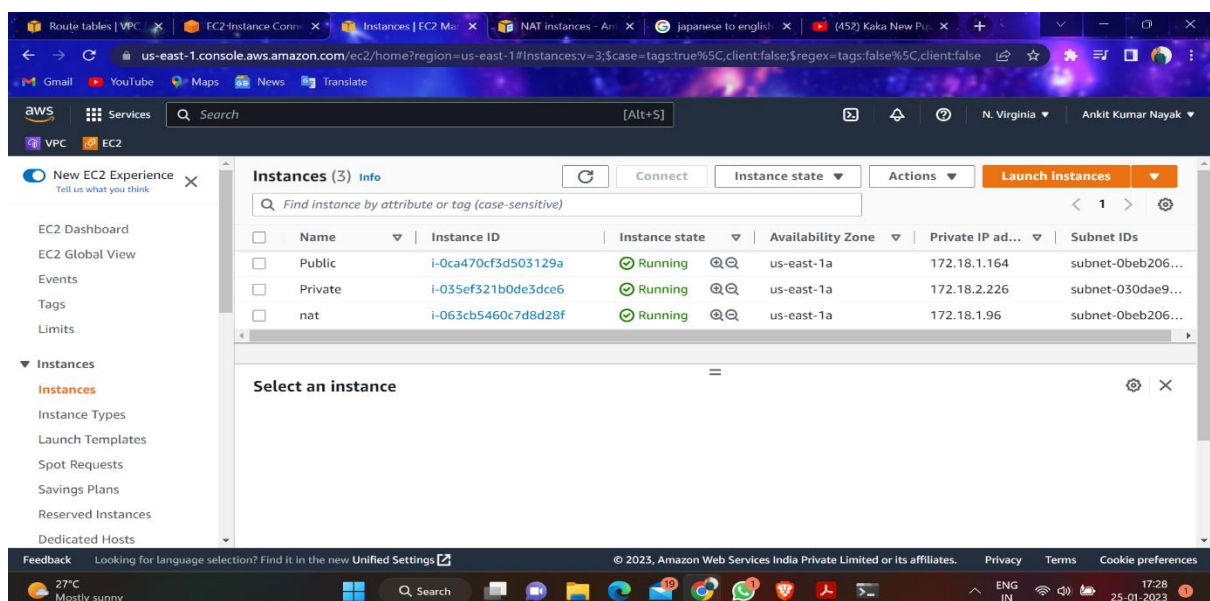
Buttons: Add route, Cancel, Preview, Save changes

7-Creating Internet Gateway



8-Creating Instances

- Create 3 separate instance
 - Public vm with public address enable, and security group with ssh and all icmp - ipv4.
 - Private vm with no public address, and security group with ssh and all icmp - ipv4.
 - Nat vm with public address enable, and security group with ssh,http,https,all icmp – ipv4.



9-Inside Nat Security Group

The screenshot displays the AWS Management Console's 'Inbound rules' page for a security group. The page lists four rules with their respective IDs, types, protocols, port ranges, and sources. The 'Source' column for each rule is set to 'Custom' and includes a search bar with the IP address '172.18.2.0/24' entered. The 'Delete' button is visible for each rule.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0d018ae237643a9ba	HTTPS	TCP	443	Custom	
sgr-0697bf1c098a4d144	SSH	TCP	22	Custom	
sgr-0eb7aa43cce608840	All ICMP - IPv4	ICMP	All	Custom	
sgr-088c3be7cc84149c6	HTTP	TCP	80	Custom	

10-Way To Stop Instance

The screenshot shows the AWS Management Console's 'Instances' page. A table lists three instances: 'Public', 'Private', and 'nat'. The 'nat' instance is selected, and a context menu is open over it, showing various actions. The 'Change source/destination check' option is highlighted. The 'Instance summary' section below the table provides details for the selected instance, including its ID, public IPv4 address, private IPv4 address, and instance state.

Name	Instance ID	Instance state	Availability Zone
Public	i-0ca470cf3d503129a	Running	us-east-1a
Private	i-035ef321b0de3dce6	Running	us-east-1a
nat	i-063cb5460c7d8d28f	Running	us-east-1a

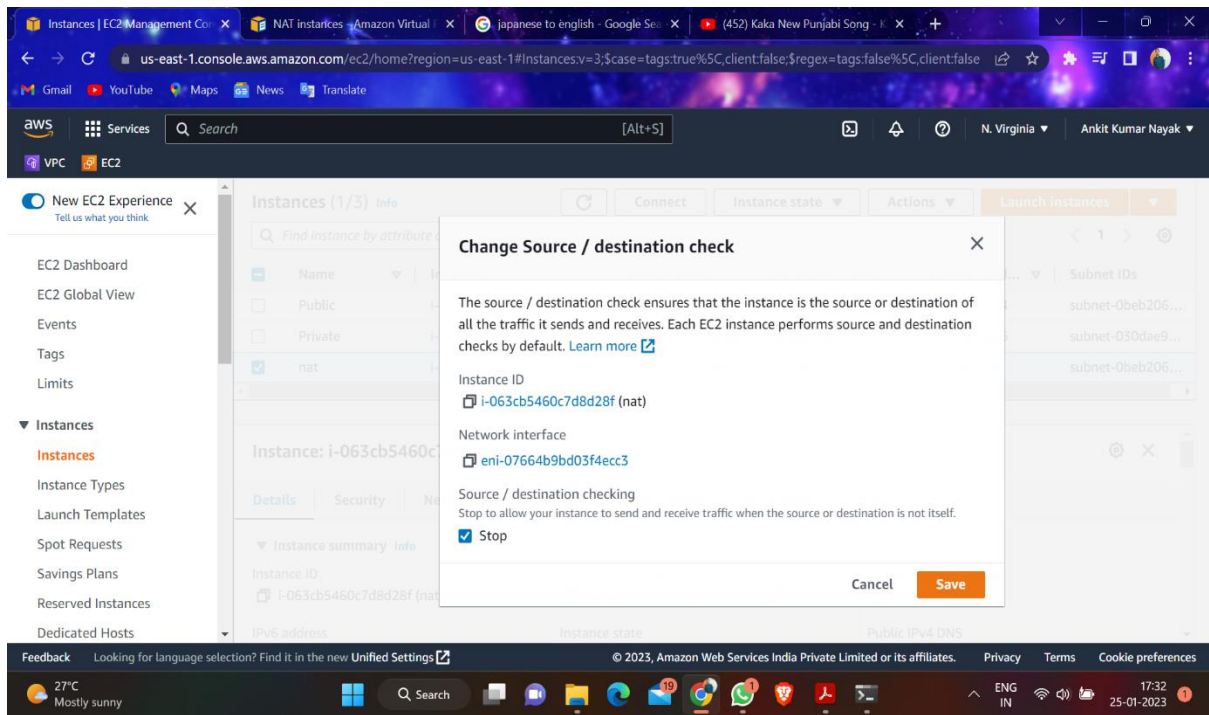
Instance: i-063cb5460c7d8d28f (nat)

Details | Security | Networking | Storage

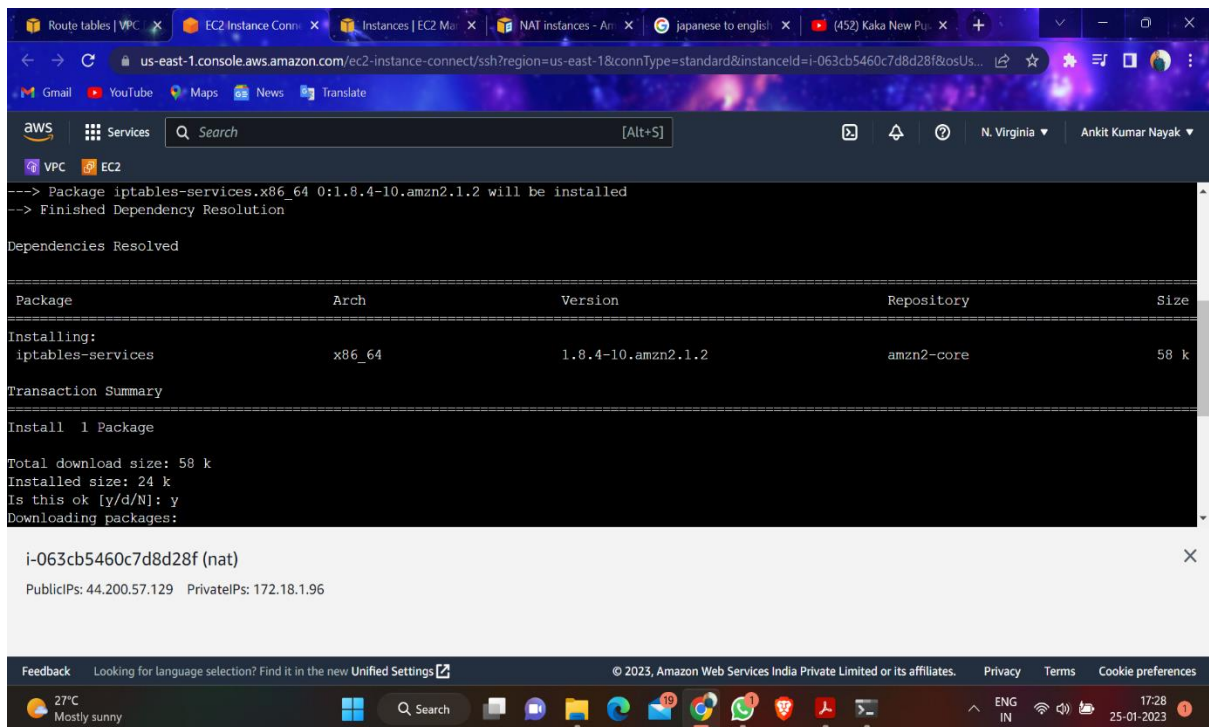
Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-063cb5460c7d8d28f (nat)	44.200.57.129 open address	172.18.1.96

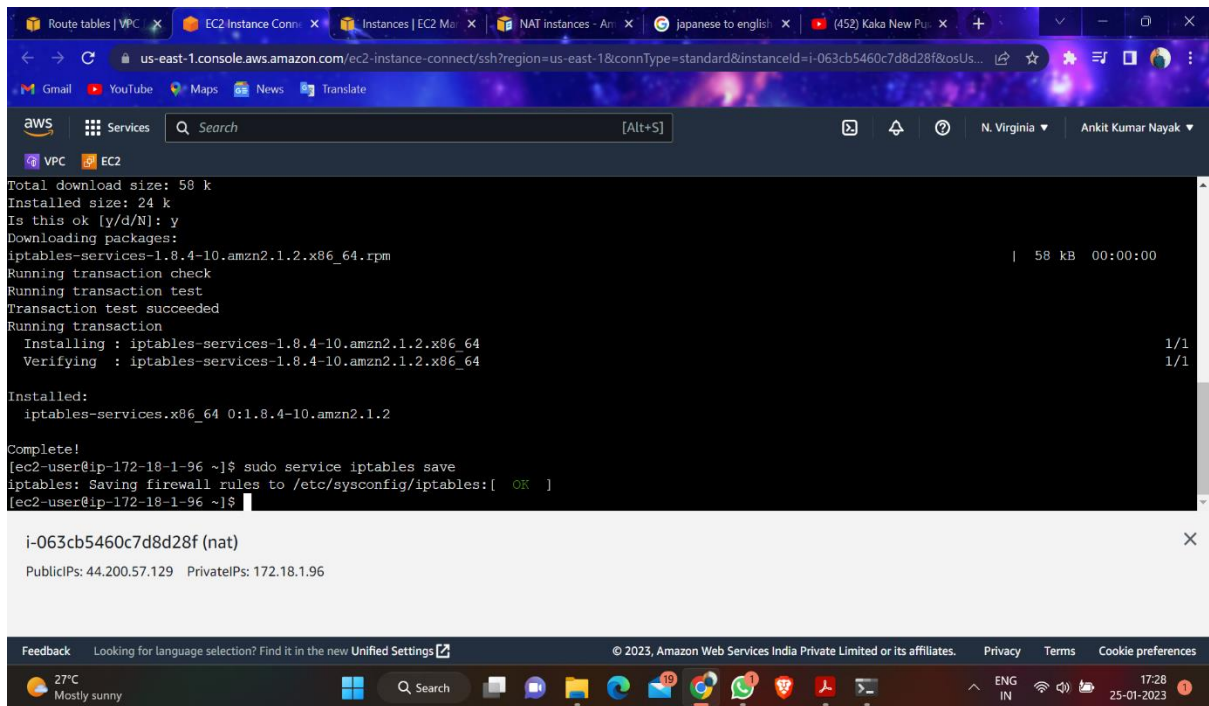
11-Scoure-Destination Check Stop



12-Installing The Packets



13-Packets Installed

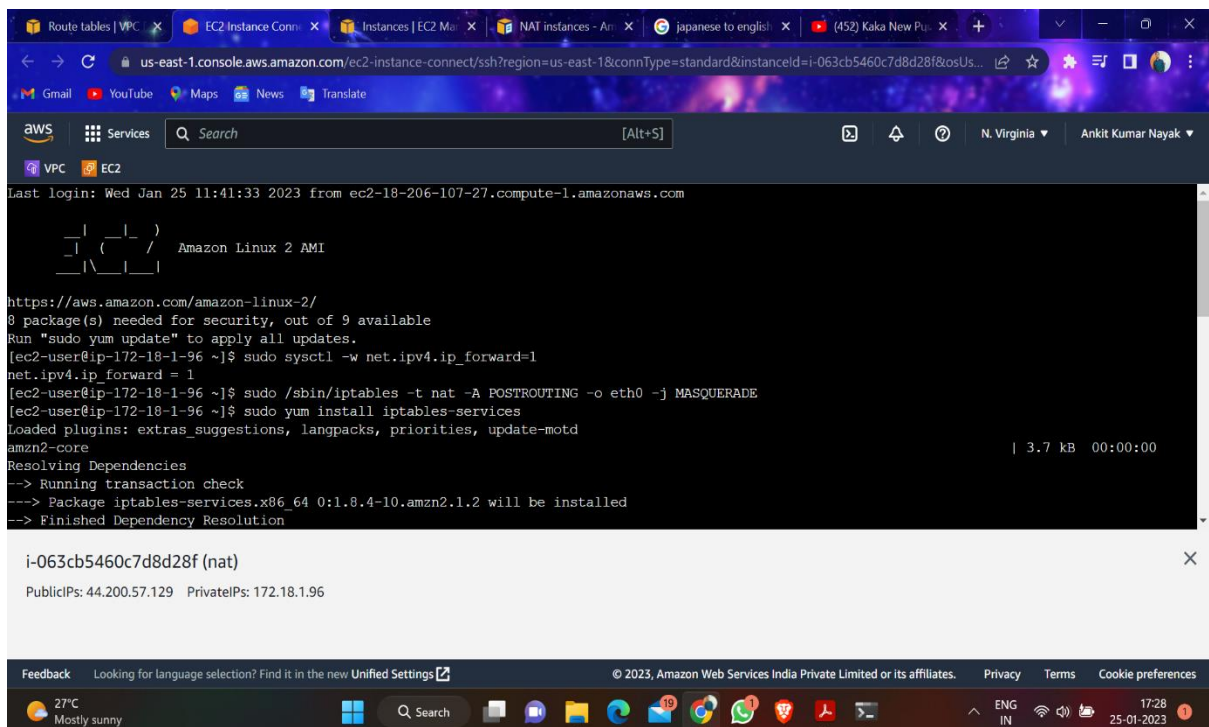


The screenshot shows the AWS Management Console with a terminal window open for an EC2 instance. The terminal output shows the installation of the `iptables-services` package. The package is downloaded (58 kB) and installed (24 kB). The installation process includes running transaction checks and a successful transaction test. The final output shows the package is installed and the service is saved.

```
Total download size: 58 k
Installed size: 24 k
Is this ok [y/d/N]: y
Downloading packages:
iptables-services-1.8.4-10.amzn2.1.2.x86_64.rpm | 58 kB 00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Installing : iptables-services-1.8.4-10.amzn2.1.2.x86_64 1/1
Verifying : iptables-services-1.8.4-10.amzn2.1.2.x86_64 1/1
Installed:
iptables-services.x86_64 0:1.8.4-10.amzn2.1.2
Complete!
[ec2-user@ip-172-18-1-96 ~]$ sudo service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
[ec2-user@ip-172-18-1-96 ~]$
```

Below the terminal window, a summary box for the instance `i-063cb5460c7d8d28f (nat)` is visible, showing Public IPs: 44.200.57.129 and Private IPs: 172.18.1.96.

14-Running Nat Instance



The screenshot shows the AWS Management Console with a terminal window open for an EC2 instance. The terminal output shows the configuration of the instance for NAT. The user runs `sudo yum update` to apply all updates. Then, they run `sudo sysctl -w net.ipv4.ip_forward=1` to enable IP forwarding. Finally, they run `sudo yum install iptables-services` to install the iptables-services package. The output shows the package is installed and the service is saved.

```
Last login: Wed Jan 25 11:41:33 2023 from ec2-18-206-107-27.compute-1.amazonaws.com
 _ _ _ _ _
 _ | ( _ ) / Amazon Linux 2 AMI
 _ | \ _ /

https://aws.amazon.com/amazon-linux-2/
0 package(s) needed for security, out of 9 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-18-1-96 ~]$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
[ec2-user@ip-172-18-1-96 ~]$ sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
[ec2-user@ip-172-18-1-96 ~]$ sudo yum install iptables-services
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core | 3.7 kB 00:00:00
Resolving Dependencies
--> Running transaction check
--> Package iptables-services.x86_64 0:1.8.4-10.amzn2.1.2 will be installed
--> Finished Dependency Resolution
```

Below the terminal window, a summary box for the instance `i-063cb5460c7d8d28f (nat)` is visible, showing Public IPs: 44.200.57.129 and Private IPs: 172.18.1.96.

15-Pinging Nat Instance

```
ec2-user@ip-172-18-2-226:~$ ping google.com
PING google.com (142.251.16.138) 56(84) bytes of data.
^C
--- google.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4082ms

[ec2-user@ip-172-18-2-226 ~]$ ssh -i "psti-01.pem" ec2-user@44.200.57.129
Warning: Identity file psti-01.pem not accessible: No such file or directory.
^C

[ec2-user@ip-172-18-2-226 ~]$ ping google.com
PING google.com (142.251.16.113) 56(84) bytes of data.
^C
--- google.com ping statistics ---
82 packets transmitted, 0 received, 100% packet loss, time 82932ms

[ec2-user@ip-172-18-2-226 ~]$ ping google.com
PING google.com (142.251.16.102) 56(84) bytes of data.
^C
--- google.com ping statistics ---
51 packets transmitted, 0 received, 100% packet loss, time 51185ms

[ec2-user@ip-172-18-2-226 ~]$ ping google.com
PING google.com (142.251.16.101) 56(84) bytes of data.
64 bytes from bl-in-f101.1e100.net (142.251.16.101): icmp_seq=167 ttl=51 time=2.19 ms
64 bytes from bl-in-f101.1e100.net (142.251.16.101): icmp_seq=168 ttl=51 time=2.87 ms
64 bytes from bl-in-f101.1e100.net (142.251.16.101): icmp_seq=169 ttl=51 time=3.09 ms
64 bytes from bl-in-f101.1e100.net (142.251.16.101): icmp_seq=170 ttl=51 time=2.04 ms
^C
--- google.com ping statistics ---
170 packets transmitted, 4 received, 97% packet loss, time 172987ms
rtt min/avg/max/mdev = 2.043/2.551/3.096/0.444 ms
```