IPv4 to IPv6 modernization Journey

Note1: The intent of our journey is not to restructure the existing architecture; it is to enhance the current architecture to support IPv6 enablement.

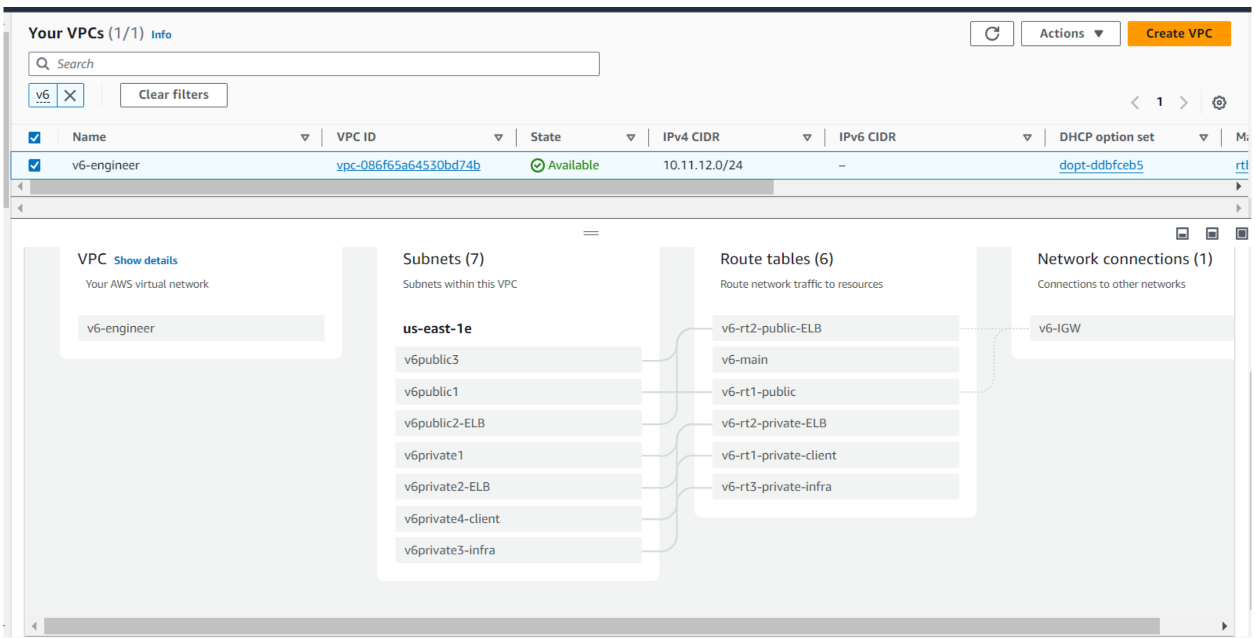
Note2: The M3 instance type does not support IPv6 connectivity. According to the AWS documentation, only the current generation instance types launched into IPv6-only subnets will have IPv6 addresses assigned. Some older instance types like M1, M2, M3, C1 and t1 do not support IPv6

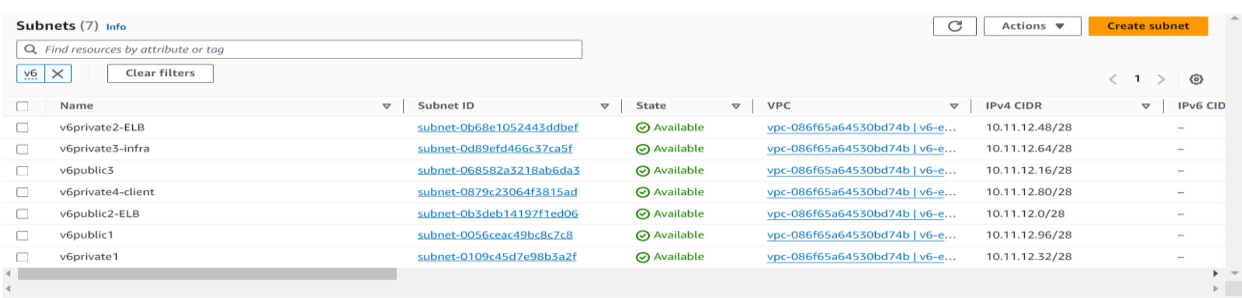
I would recommend testing with a newer t2.small or t3.micro instance type as those generally have better performance and are confirmed to support IPv6.

Link1: Which EC2 types support IPv6?

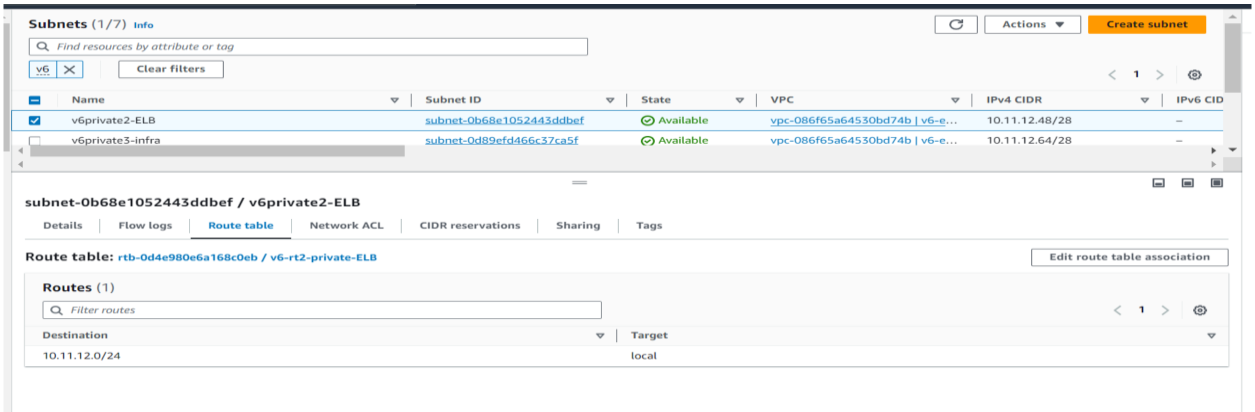
Link2: AWS services that support IPv6 - Amazon Virtual Private Cloud

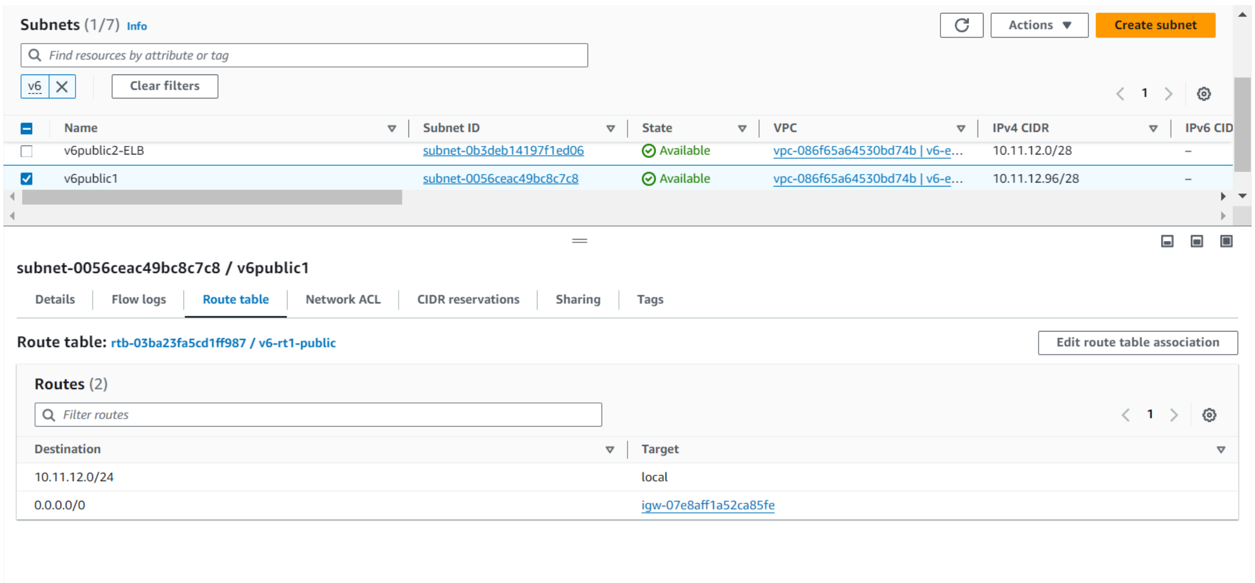
Link3: Instance types - Amazon Elastic Compute Cloud

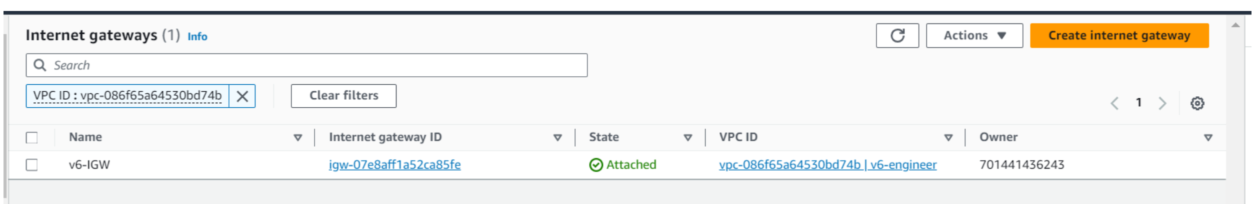




Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CID
v6private2-ELB	subnet-0b68e1052443ddbef	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.48/28	–
v6private3-infra	subnet-0d89efd466c37ca5f	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.64/28	–
v6public3	subnet-068582a3218ab6da3	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.16/28	–
v6private4-client	subnet-0879c23064f3815ad	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.80/28	–
v6public2-ELB	subnet-0b3deb14197f1ed06	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.0/28	–
v6public1	subnet-0056ceac49bc8c7c8	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.96/28	–
v6private1	subnet-0109c45d7e98b3a2f	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.32/28	–







- The Internet Gateway (IGW) is not a focal point in this scenario. When your subnet consists solely of IPv6 addresses, the Egress-Only Internet Gateway must be used.

You have successfully updated subnet associations for acl-098d779793f5e3627 / v6-private-client.

Details

Network ACLs (1/2) Info

Actions | Create network ACL

Find resources by attribute or tag

VPC ID : vpc-086f65a64530bd74b | Clear filters

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
v6-main	acl-07a0b3eca63e0a143	6 Subnets	Yes	vpc-086f65a64530bd74b / v6-engineer	2 Inbound rules
v6-private-client	acl-098d779793f5e3627	subnet-0879c23064f3815ad / v6private4-client	No	vpc-086f65a64530bd74b / v6-engineer	1 Inbound rule

acl-098d779793f5e3627 / v6-private-client

Details | Inbound rules | Outbound rules | Subnet associations | Tags

Subnet associations (1)

Edit subnet associations

Filter subnet associations

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IPv6 CIDR
v6private4-client	subnet-0879c23064f3815ad	acl-098d779793f5e3627 / v6-private-c...	us-east-1e	10.11.12.80/28	–

Security Groups (13) Info

Actions | Export security groups to CSV | Create security group

Find resources by attribute or tag

vpc-086f65a64530bd74b | Clear filters

Name	Security group ID	Security group name	VPC ID	Description
v6-default	sg-0e7f89ac0e208a415	default	vpc-086f65a64530bd74b	default VPC security group
v6sg9	sg-059bb88a6db874bc3	v6sg9	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg12-linux	sg-0263f312bfaaee7de	v6sg12-linux	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg2	sg-05bfeda01e00dbdd5	v6sg2	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg6	sg-08ffb6a0d5f202cf3	v6sg6	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg11-linux	sg-0538e0693c5093fbe	v6sg11-linux	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg3	sg-05746bd881c250d3f	v6sg3	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg1	sg-0fdf7bf95108ae234	v6sg1	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg8	sg-07e98d00de63fe97c	v6sg8	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg7	sg-0d0b758ff6d351c4c	v6sg7	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg4	sg-022d3724a5fd6a6de	v6sg4	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg5	sg-074541009ab35d56a	v6sg5	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...
v6sg10	sg-06bb2a4399aebae79	v6sg10	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...

Security Groups (1/13) Info

Actions | Export security groups to CSV | Create security group

Find resources by attribute or tag

vpc-086f65a64530bd74b | Clear filters

Name	Security group ID	Security group name	VPC ID	Description
v6-default	sg-0e7f89ac0e208a415	default	vpc-086f65a64530bd74b	default VPC security group
v6sg9	sg-059bb88a6db874bc3	v6sg9	vpc-086f65a64530bd74b	launch-wizard-16 created 2024-01-28...

sg-0e7f89ac0e208a415 - default

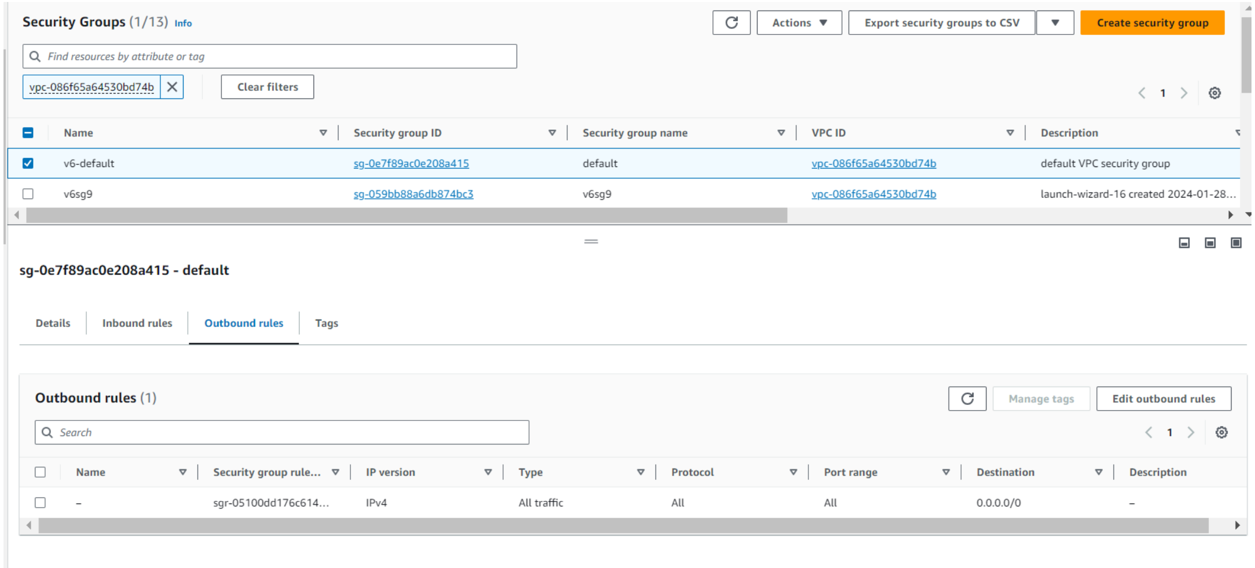
Details | Inbound rules | Outbound rules | Tags

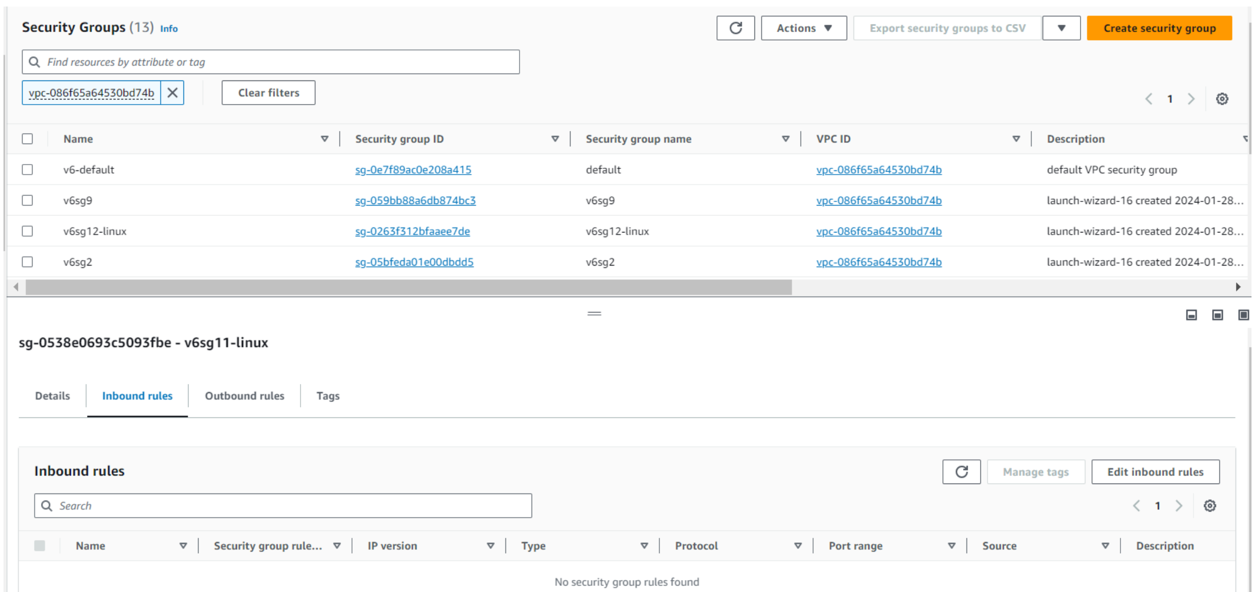
Inbound rules (1)

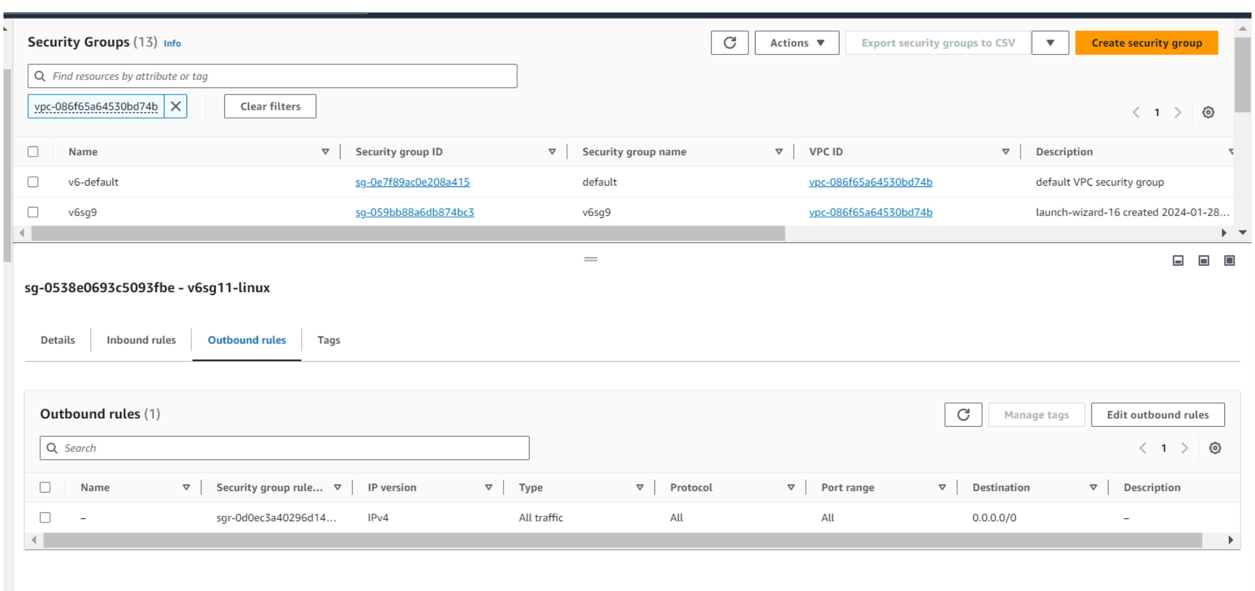
Manage tags | Edit inbound rules

Search

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
–	sgr-05caceacbb6626682	–	All traffic	All	All	sg-0e7f89ac0e208a41...	–

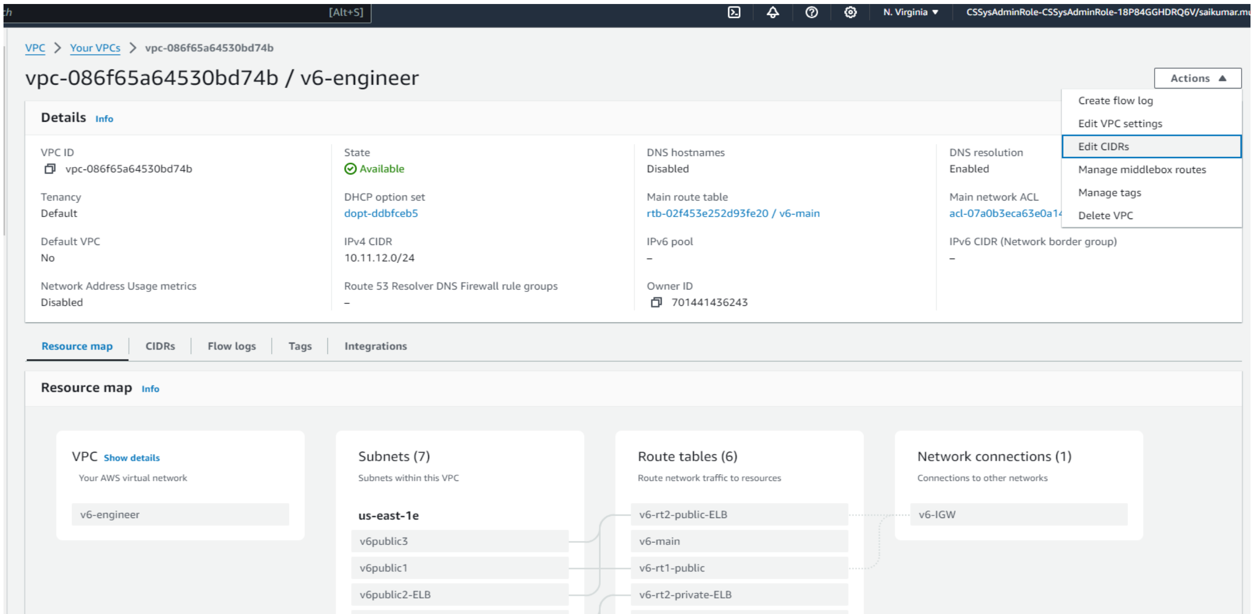

Security Groups (1/13) Info
Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
vpc-086f65a64530bd74b
Clear filters
Name
Security group ID
Security group name
VPC ID
Description
v6-default
sg-0e7f89ac0e208a415
default
vpc-086f65a64530bd74b
default VPC security group
v6sg9
sg-059bb88a6db874bc3
v6sg9
vpc-086f65a64530bd74b
launch-wizard-16 created 2024-01-28...
sg-0e7f89ac0e208a415 - default
Details
Inbound rules
Outbound rules
Tags
Outbound rules (1)
Manage tags
Edit outbound rules
Search
Name
Security group rule...
IP version
Type
Protocol
Port range
Destination
Description
–
sgr-05100dd176c614...
IPv4
All traffic
All
All
0.0.0.0/0
–

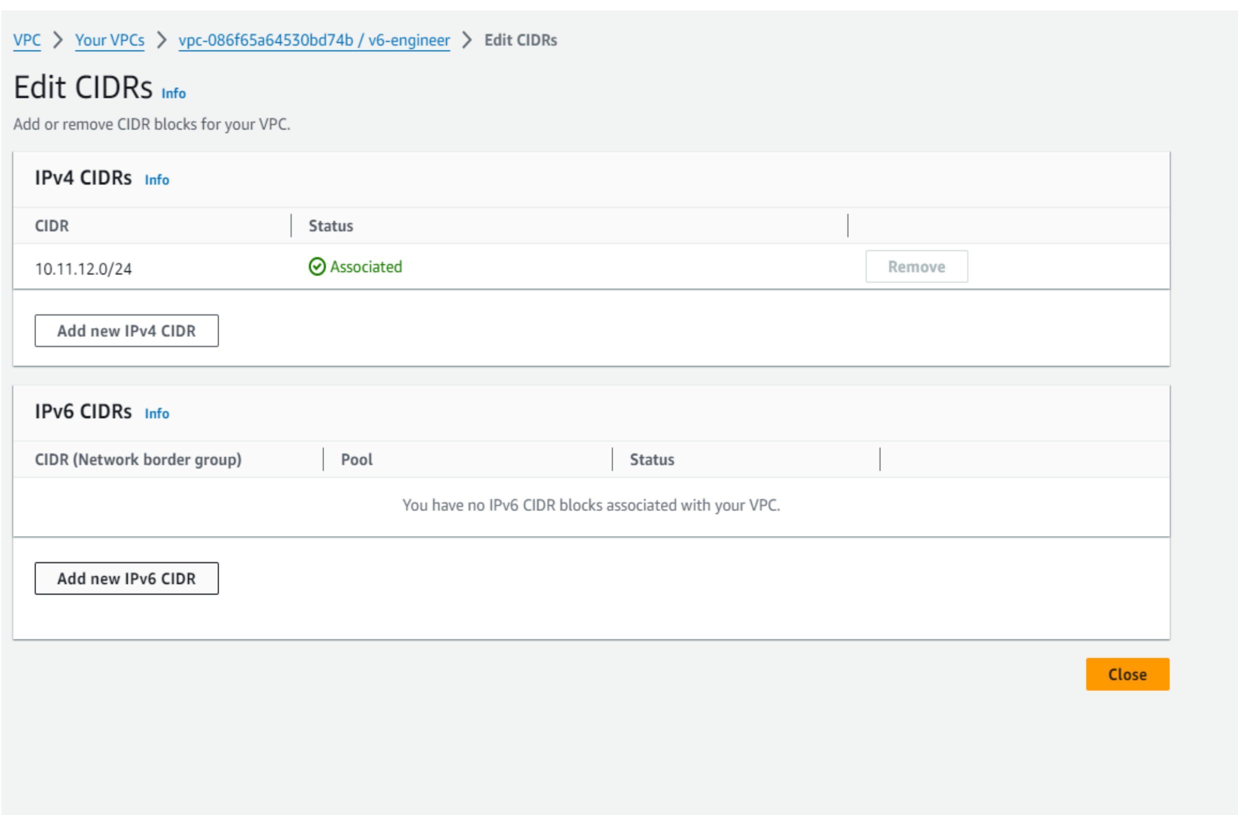

Security Groups (13) Info
Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
vpc-086f65a64530bd74b
Clear filters
Name
Security group ID
Security group name
VPC ID
Description
v6-default
sg-0e7f89ac0e208a415
default
vpc-086f65a64530bd74b
default VPC security group
v6sg9
sg-059bb88a6db874bc3
v6sg9
vpc-086f65a64530bd74b
launch-wizard-16 created 2024-01-28...
v6sg12-linux
sg-0263f312bfaaee7de
v6sg12-linux
vpc-086f65a64530bd74b
launch-wizard-16 created 2024-01-28...
v6sg2
sg-05bfeda01e00dbdd5
v6sg2
vpc-086f65a64530bd74b
launch-wizard-16 created 2024-01-28...
sg-0538e0693c5093fbe - v6sg11-linux
Details
Inbound rules
Outbound rules
Tags
Inbound rules
Manage tags
Edit inbound rules
Search
Name
Security group rule...
IP version
Type
Protocol
Port range
Source
Description
No security group rules found

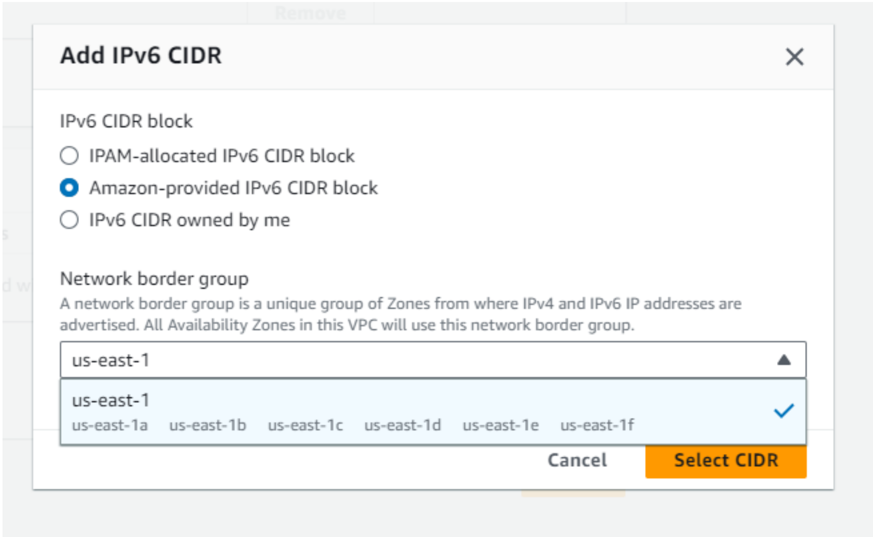

Security Groups (13) Info
Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
vpc-086f65a64530bd74b
Clear filters
Name
Security group ID
Security group name
VPC ID
Description
v6-default
sg-0e7f89ac0e208a415
default
vpc-086f65a64530bd74b
default VPC security group
v6sg9
sg-059bb88a6db874bc3
v6sg9
vpc-086f65a64530bd74b
launch-wizard-16 created 2024-01-28...
sg-0538e0693c5093fbe - v6sg11-linux
Details
Inbound rules
Outbound rules
Tags
Outbound rules (1)
Manage tags
Edit outbound rules
Search
Name
Security group rule...
IP version
Type
Protocol
Port range
Destination
Description
–
sgr-0d0ec3a40296d14...
IPv4
All traffic
All
All
0.0.0.0/0
–

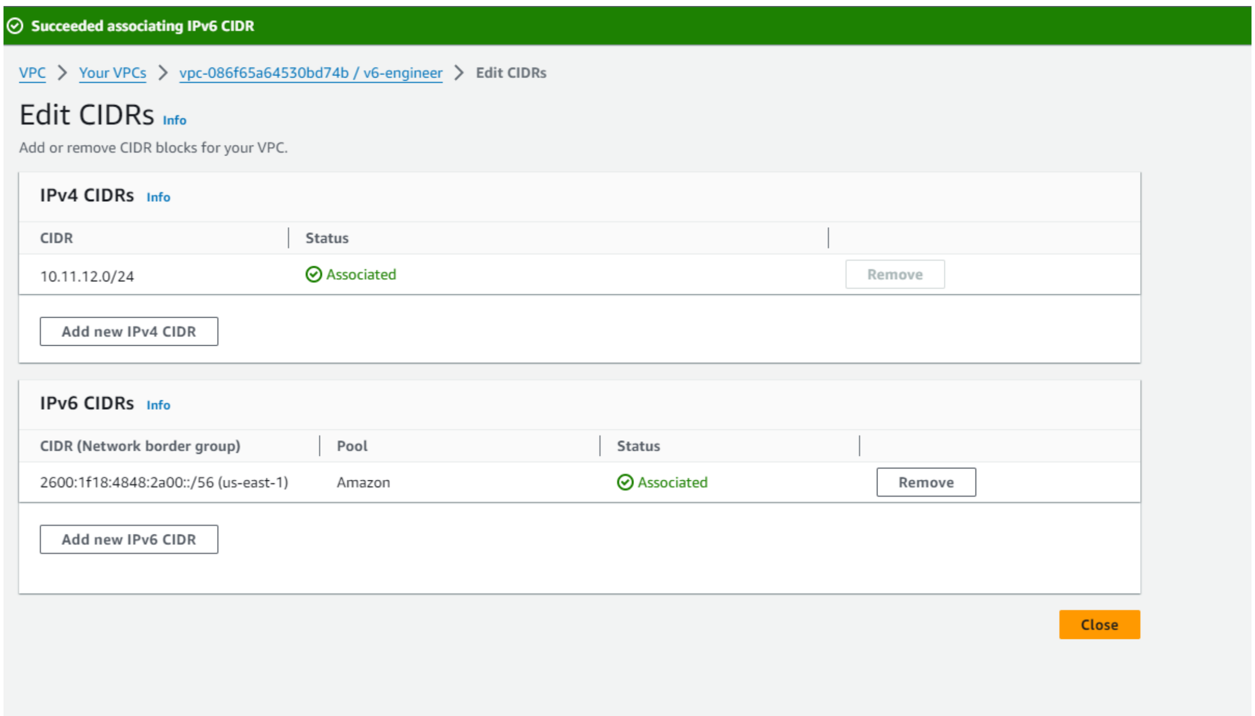
Note: Observe carefully: the default Security Group (created during VPC creation) has both inbound and outbound rules. In contrast, Security Groups created during instance creation will have rules only for outbound traffic, not for inbound traffic.

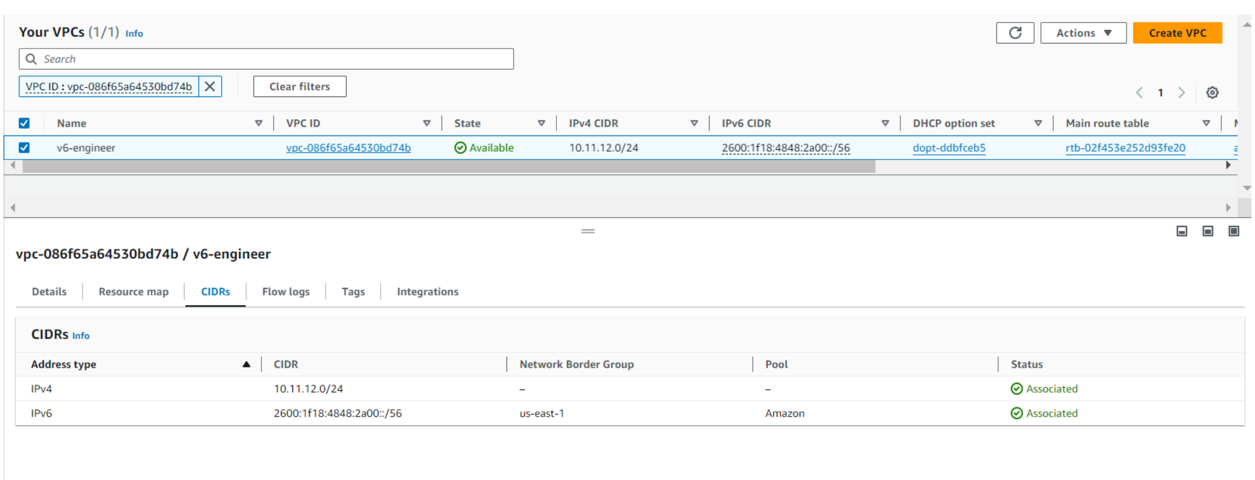
Above all, before IPv6 is enabled. Now, the changes below represent what will be observed after IPv6 is enabled on top of the VPC first.






Add IPv6 CIDR
IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Network border group
A network border group is a unique group of Zones from where IPv4 and IPv6 IP addresses are advertised. All Availability Zones in this VPC will use this network border group.
us-east-1
us-east-1
us-east-1a us-east-1b us-east-1c us-east-1d us-east-1e us-east-1f
Cancel
Select CIDR


Succeeded associating IPv6 CIDR
VPC > Your VPCs > vpc-086f65a64530bd74b / v6-engineer > Edit CIDRs
Edit CIDRs Info
Add or remove CIDR blocks for your VPC.
IPv4 CIDRs Info
CIDR
Status
10.11.12.0/24
Associated
Remove
Add new IPv4 CIDR
IPv6 CIDRs Info
CIDR (Network border group)
Pool
Status
2600:1f18:4848:2a00::/56 (us-east-1)
Amazon
Associated
Remove
Add new IPv6 CIDR
Close


Your VPCs (1/1) Info
Actions
Create VPC
Search
VPC ID : vpc-086f65a64530bd74b
Clear filters
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP option set
Main route table
v6-engineer
vpc-086f65a64530bd74b
Available
10.11.12.0/24
2600:1f18:4848:2a00::/56
dopt-ddbfceb5
rtb-02f453e252d93fe20
vpc-086f65a64530bd74b / v6-engineer
Details
Resource map
CIDRs
Flow logs
Tags
Integrations
CIDRs Info
Address type
CIDR
Network Border Group
Pool
Status
IPv4
10.11.12.0/24
–
–
Associated
IPv6
2600:1f18:4848:2a00::/56
us-east-1
Amazon
Associated

The above screenshots represents the IPv6 enabled on VPC .. now lets enable at each subnet level.. lets try to do so math calculations for the IPv4 address ranges that we have assigned to VPC and subnet as per our test scenario.

IPv4 CIDR for VPC is /24 no of equal subnets that we can divide or no of IP address that are available for this range would be 32-24 = 8. Now, 2**8 = 256 (256 IP address are available for /24 CIDR)..

Similarly, each subnet we specified /28 as our CIDR. 32-28=4. Now, 2**4=16

With respect to AWS cloud provider if you are spinning up any resource within any of the created subnet the first 4 and the last one IP will be always reserved for AWS for its computational services. Let say, 10.11.12.48/28 is IP CIDR..

The CIDR notation "10.11.12.48/28" represents a subnet with a prefix length of 28 bits. In IPv4, a /28 subnet means that the first 28 bits are the network part, and the remaining 4 bits are used for host addresses.

The formula to calculate the number of available IP addresses in a subnet is 2^(32 - prefix length).

For "/28", the calculation is 2^(32 - 28) = 2^4 = 16.

So, there are 16 IP addresses available in the subnet "10.11.12.48/28". The range of IP addresses can be determined by considering the increment of 1 for each host address within the subnet. The usable IP addresses typically range from the first address (network address) to the last address (broadcast address) in the subnet.

Here are the IP addresses in the subnet "10.11.12.48/28":

Network Address: 10.11.12.48

Usable IP addresses: 10.11.12.49 to 10.11.12.62

Broadcast Address: 10.11.12.63

So, there are 16 IP addresses in total, ranging from 10.11.12.48 to 10.11.12.63. but, (.48,.49,.50,.51 and .63) not available to get assigned to our resource and in between any one IP will get associated to our resource.

Let's revisit IPv6. The reason I mentioned IPv4 earlier is due to our IP address management practices, where we don't necessarily use contiguous ranges. Even though our VPC can accommodate 16 equal /28 subnets, we have currently created only 7 subnets with /28, reserving the possibility to create more in the future if needed. Similarly, we aim to calculate for IPv6. As we are aware, the IPv6 CIDR for our VPC is /56, providing approximately 4,722,366,482,869,645,213,696 IPs, nearly five quintillion, which is an immensely vast address space.

This is AWS given IPv6 (2600:1f18:4848:2a00::/56)

In simply let me try to explain you how IPv6 works before we enable it on subnet level.

<u>Note:</u> As per IPv6 architectural design, In IPv6, the minimum and maximum CIDR prefix lengths are determined by the available address space. Unlike IPv4, where subnets are often allocated in powers of 2, IPv6 subnets are typically allocated with a fixed prefix length of /64 due to the vast address space available.

The /64 prefix length is considered the standard and recommended for IPv6 subnets. This is because IPv6 was designed with a huge address space, and a /64 subnet provides an ample 2^64 addresses, which is more than enough for most purposes.

The /64 recommendation comes from considerations related to IPv6's Stateless Address Autoconfiguration (SLAAC) and Neighbor Discovery Protocol. Using a /64 allows for efficient address autoconfiguration and simplifies network operations.

While technically possible, using shorter or longer prefixes (e.g., /60, /56, /48) for subnets in IPv6 is not recommended and can lead to operational challenges. Allocating anything smaller than /64 subnets breaks some fundamental features of IPv6.

So, in IPv6, the standard practice is to use /64 as the minimum and maximum CIDR prefix length for subnets.

Question: Then considering minimum and maximum /64 for subnet, how many equal sized /64 subnets can we divide from /56 VPC?

Answer: In IPv6, a /56 is a 56-bit address block. To determine the number of /64 subnets you can have within a /56 VPC, you can use the formula:

Number of /64 subnets=2~(64−56)

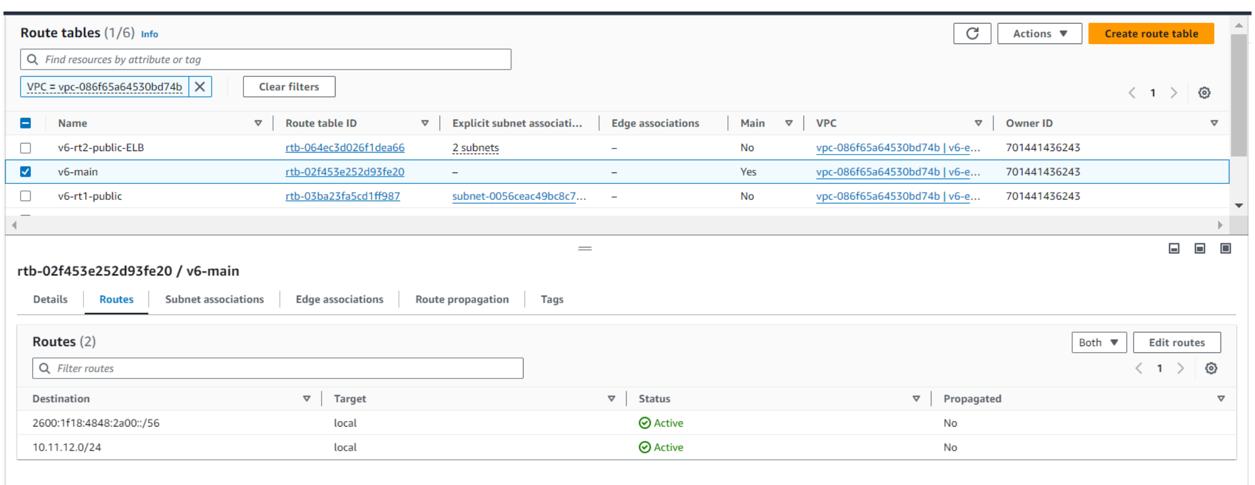
Here's the calculation:

Number of /64 subnets=28=256Number of /64 subnets=28=256

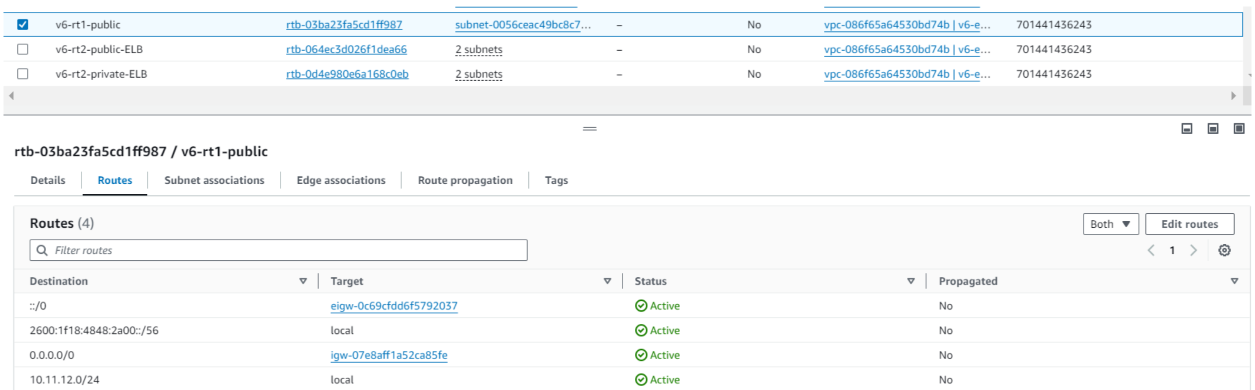
So, within a /56 VPC, you can have 256 equal-sized /64 subnets. Each /64 subnet within the /56 will have its own range of 2^64 IPv6 addresses, providing a vast number of addresses for each subnet.

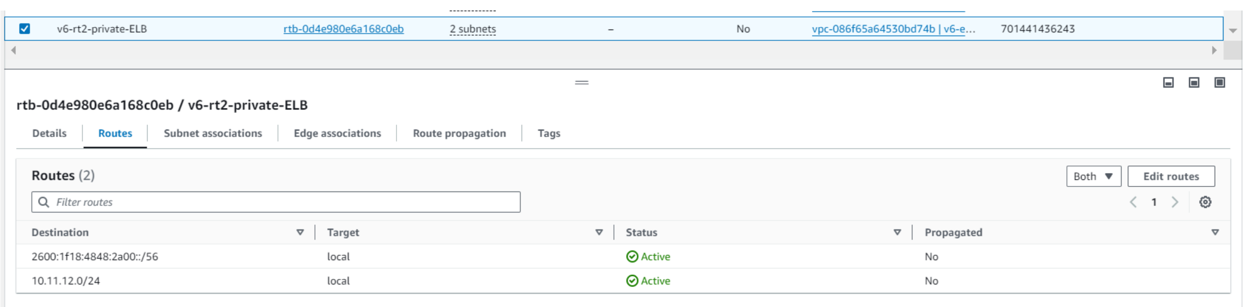
This is important to notice, once the IPv6 is enabled on VPC, will see the first changes on default and Custom Route Table. Both default and custom route tables with inherit the IPv6 address as local route into the tables. Let's try to understand looking into below images:

<u>1: main/default route table provisioned with VPC</u>

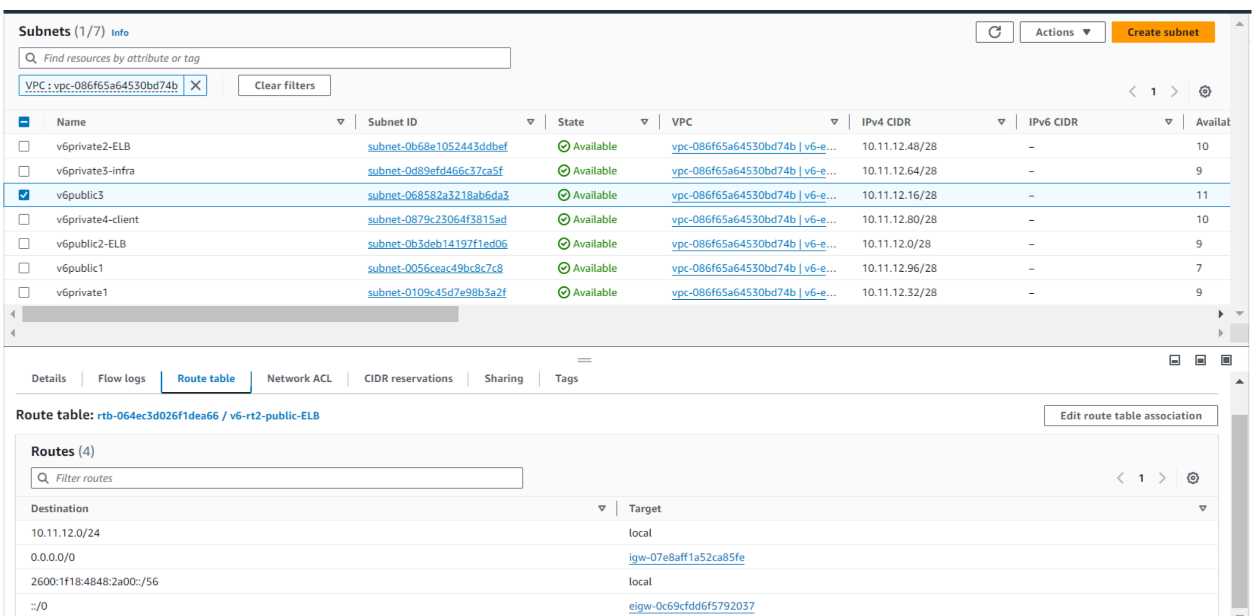


2: Custom public and private route tables





Public and Private Subnets with route tables association and this is how they look:



Subnets (1/7) Info

Actions ▼ | Create subnet

Find resources by attribute or tag

VPC : vpc-086f65a64530bd74b | Clear filters

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Availat
v6private2-ELB	subnet-0b68e1052443ddbef	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.48/28	–	10
v6private3-infra	subnet-0d89efd466c37ca5f	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.64/28	–	9
v6public3	subnet-068582a3218ab6da3	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.16/28	–	11
v6private4-client	subnet-0879c23064f3815ad	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.80/28	–	10
v6public2-ELB	subnet-0b3deb14197f1ed06	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.0/28	–	9
v6public1	subnet-0056ceac49bc8c7c8	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.96/28	–	7
v6private1	subnet-0109c45d7e98b3a2f	Available	vpc-086f65a64530bd74b | v6-e...	10.11.12.32/28	–	9

subnet-0879c23064f3815ad / v6private4-client

Details | Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Route table: rtb-0406e45d7031d3aca / v6-rt1-private-client

Edit route table association

Routes (2)

Filter routes

Destination	Target
10.11.12.0/24	local
2600:1f18:4848:2a00::/56	local

Changes on NACL after IPv6 enabled on VPC:

Main NACL:

Inbound:

Network ACLs (1/2) Info

Actions ▼ | Create network ACL

Find resources by attribute or tag

v6 | Clear filters

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
v6-private-client	acl-098d779793f5e3627	subnet-0879c23064f3815ad / v6private4-client	No	vpc-086f65a64530bd74b / v6-engineer	2 Inbound rules	2 Outbound rules
v6-main	acl-07a0b3eca63e0a143	6 Subnets	Yes	vpc-086f65a64530bd74b / v6-engineer	4 Inbound rules	4 Outbound rules

acl-07a0b3eca63e0a143 / v6-main

Details | Inbound rules | Outbound rules | Subnet associations | Tags

Inbound rules (4)

Edit inbound rules

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	All traffic	All	All	::/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

Outbound:

v6-main	acl-07a0b3eca63e0a143	6 Subnets	Yes	vpc-086f65a64530bd74b / v6-engineer	4 Inbound rules	4 Outbound rules

acl-07a0b3eca63e0a143 / v6-main

Details | Inbound rules | Outbound rules | Subnet associations | Tags

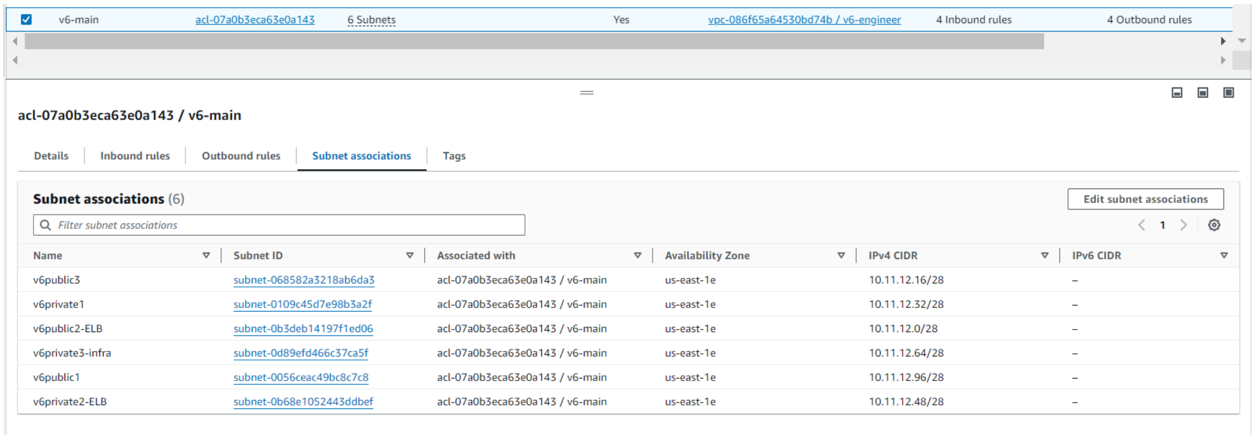
Outbound rules (4)

Edit outbound rules

Filter outbound rules

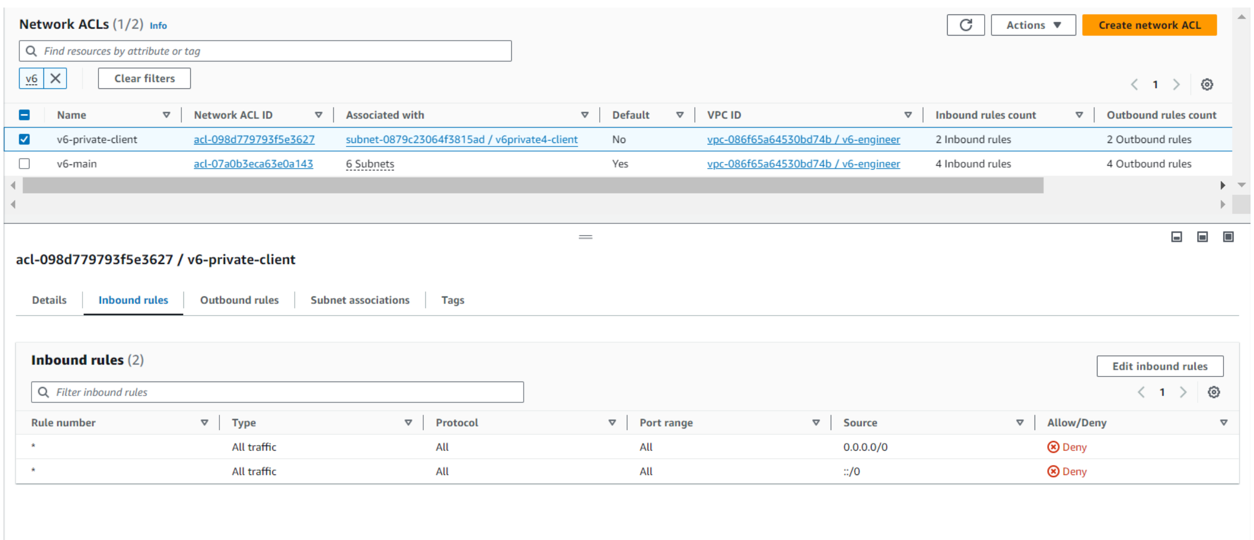
Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	All traffic	All	All	::/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

Subnet Associations on NACL before IPv6 enabled on subnet level:

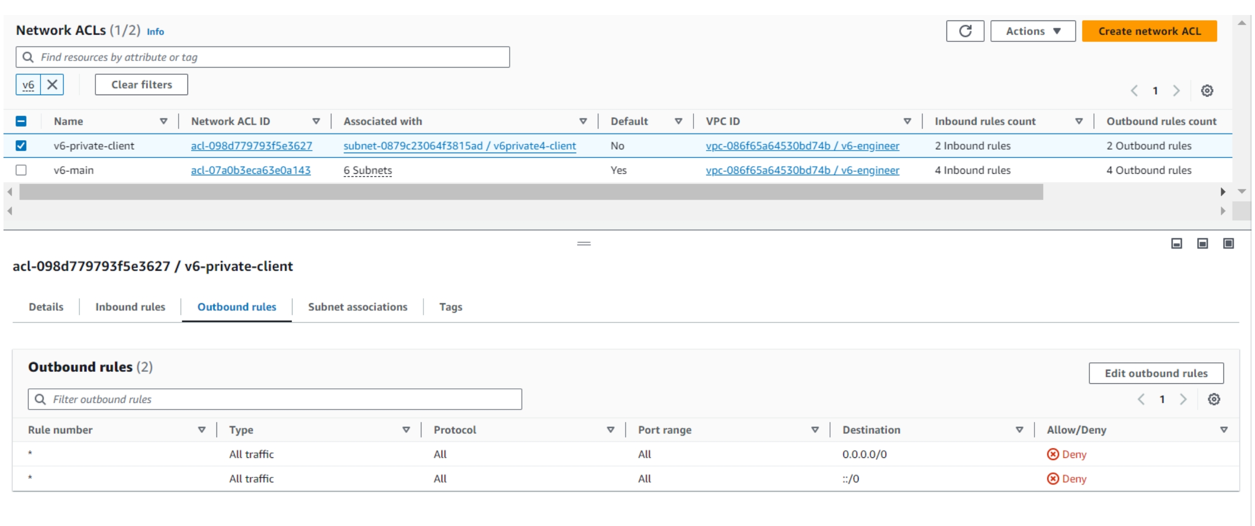


Custom NACL:

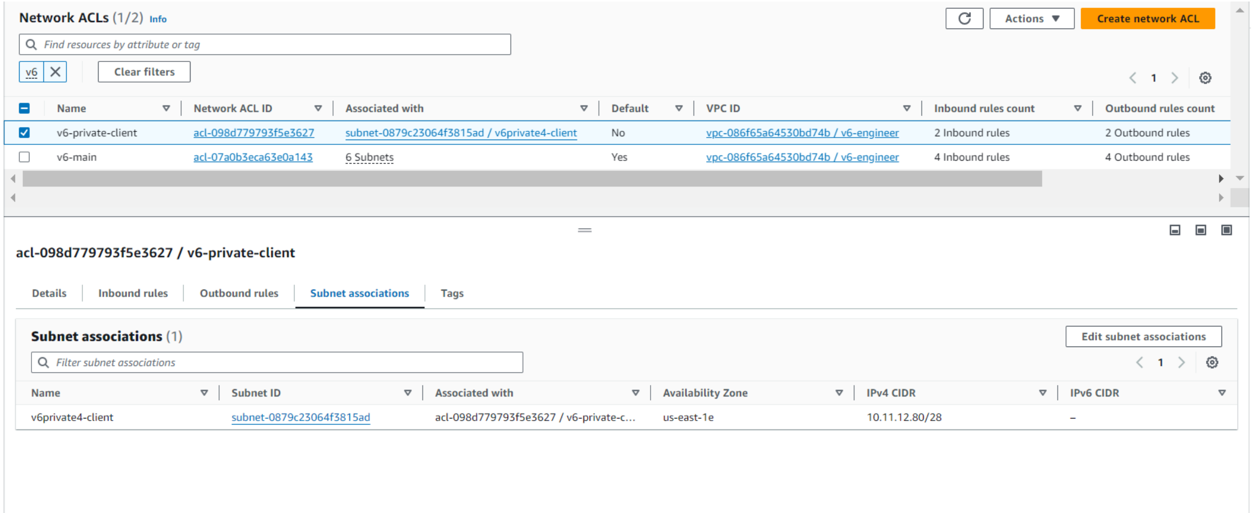
Inbound:



Outbound:

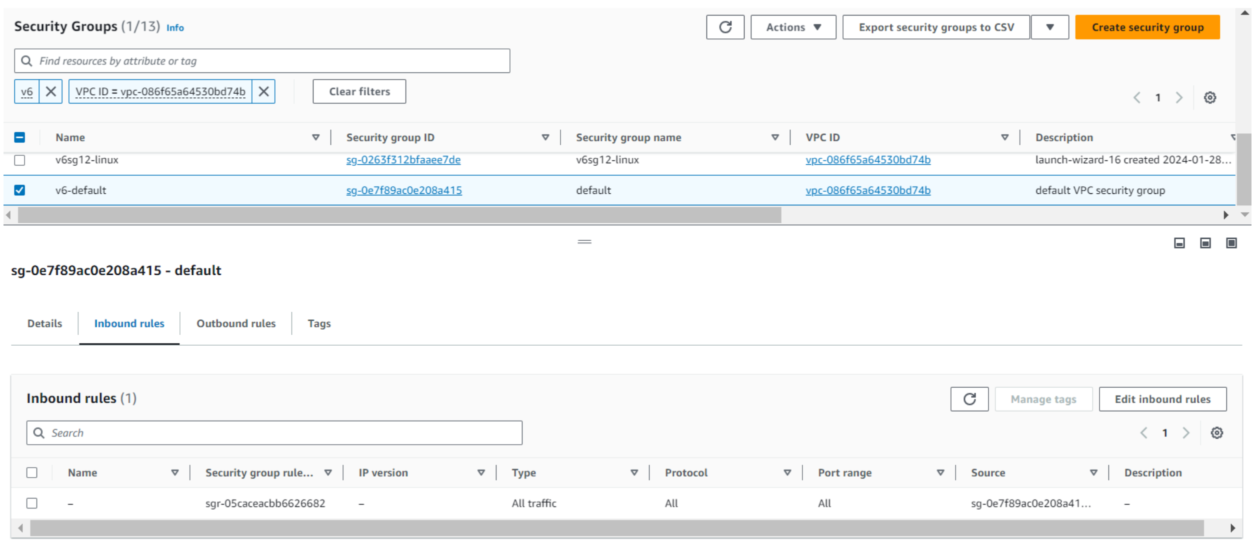


Subnet associations will see only IPv4 not IPv6 address.

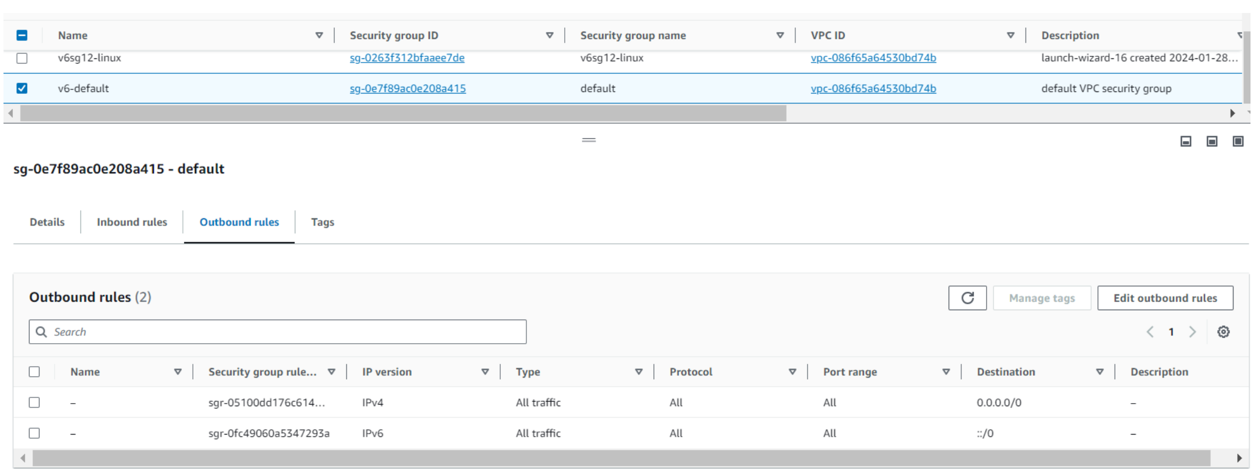


Changes on default security group of VPC and default security group of instance:

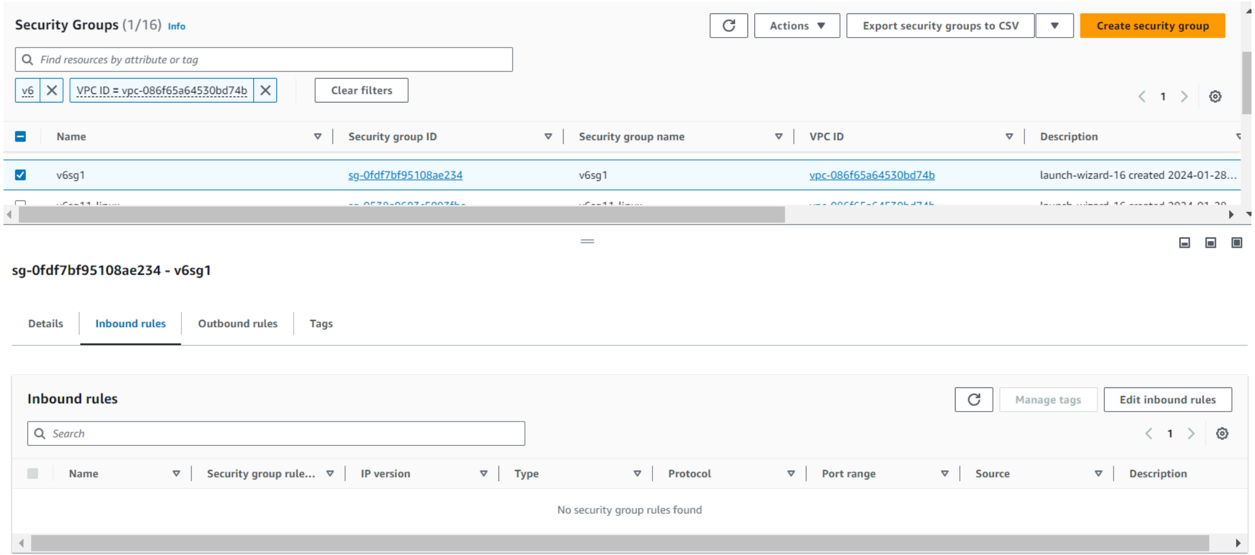
Inbound security group of VPC:



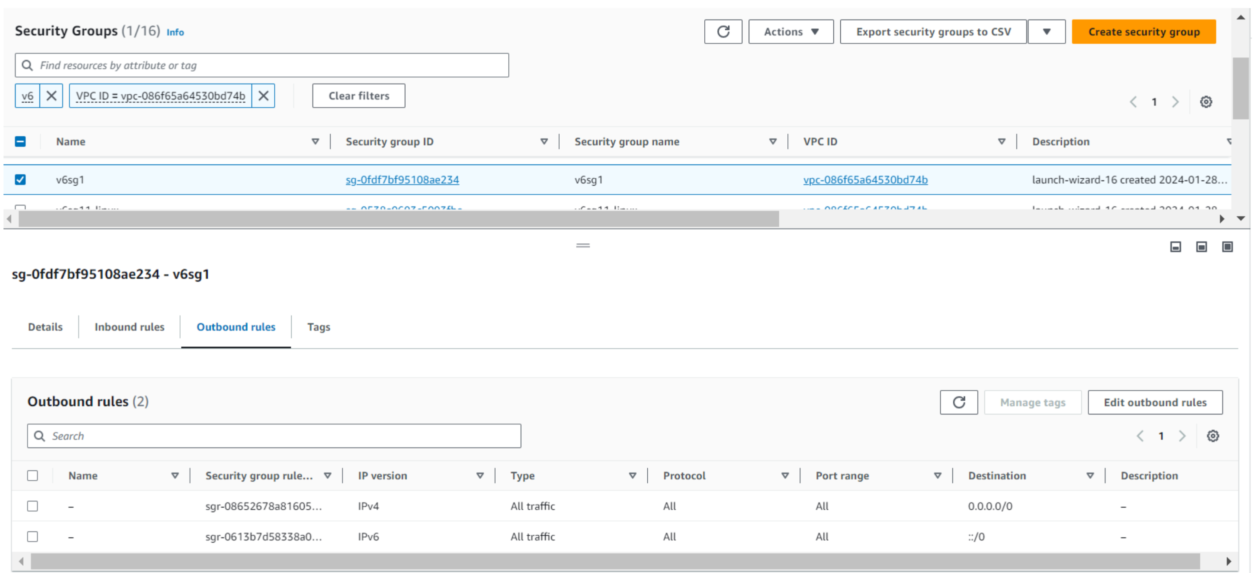
Outbound security group of VPC:



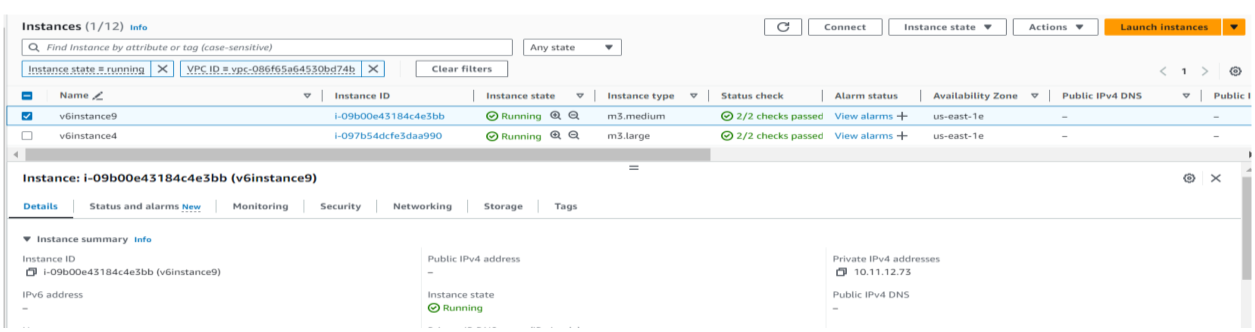
Inbound security group of instances: (No inbound rule)



Outbound security group of instances:

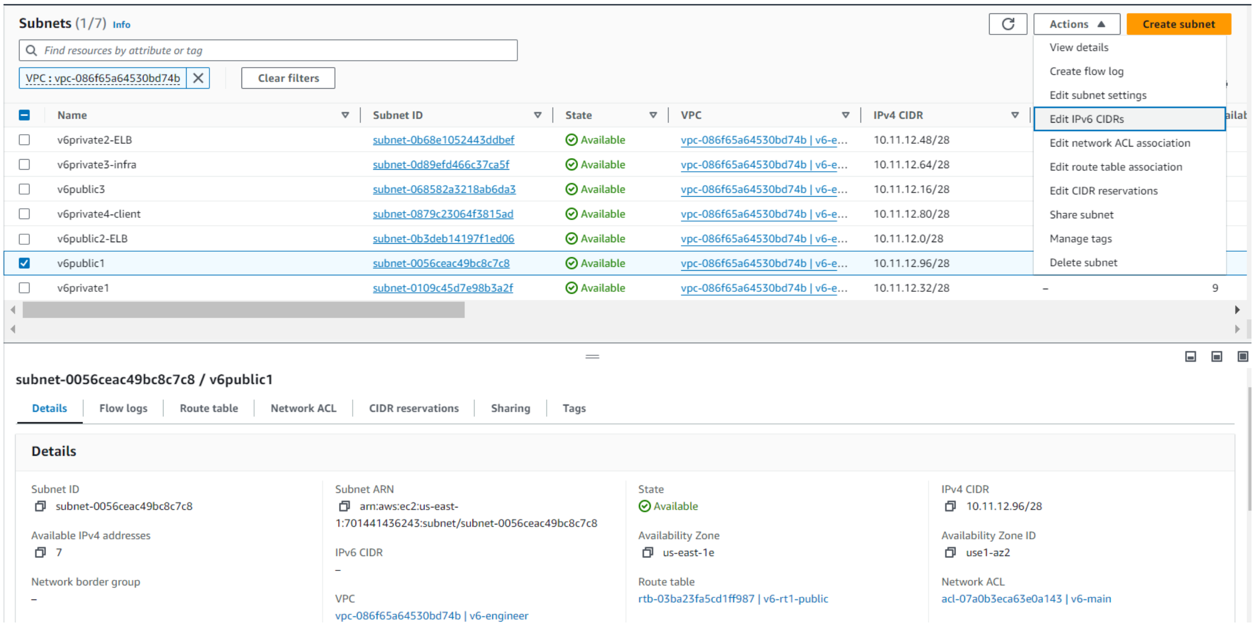


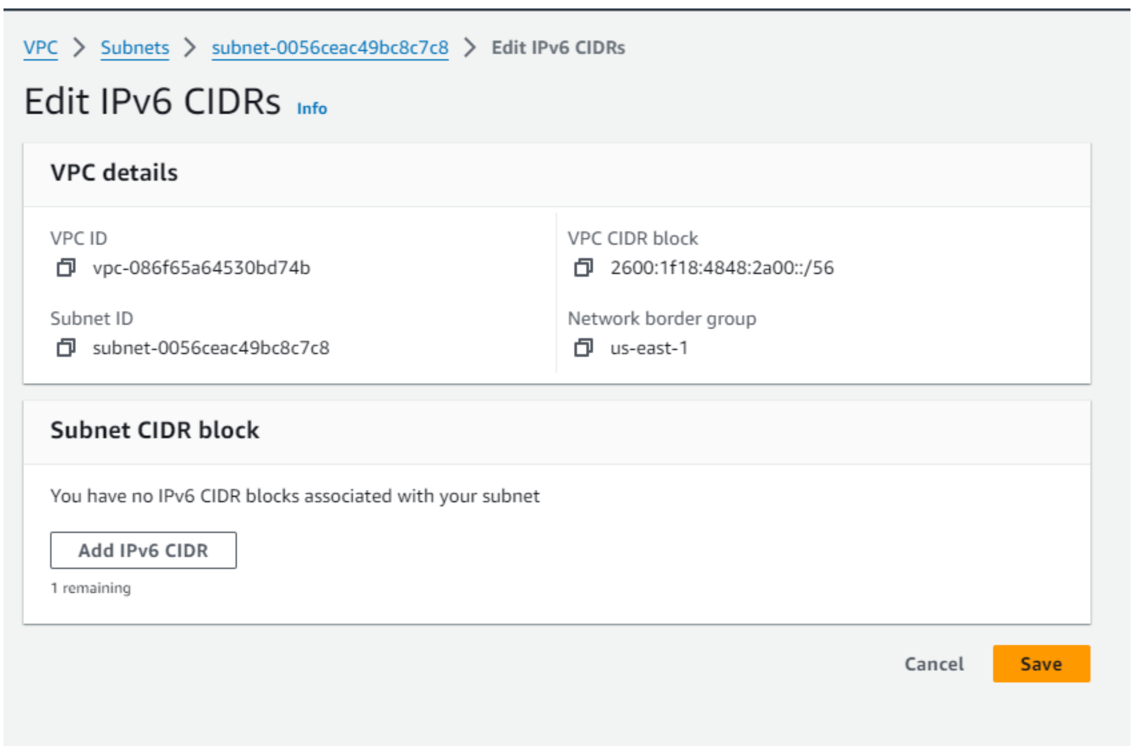
Instance:

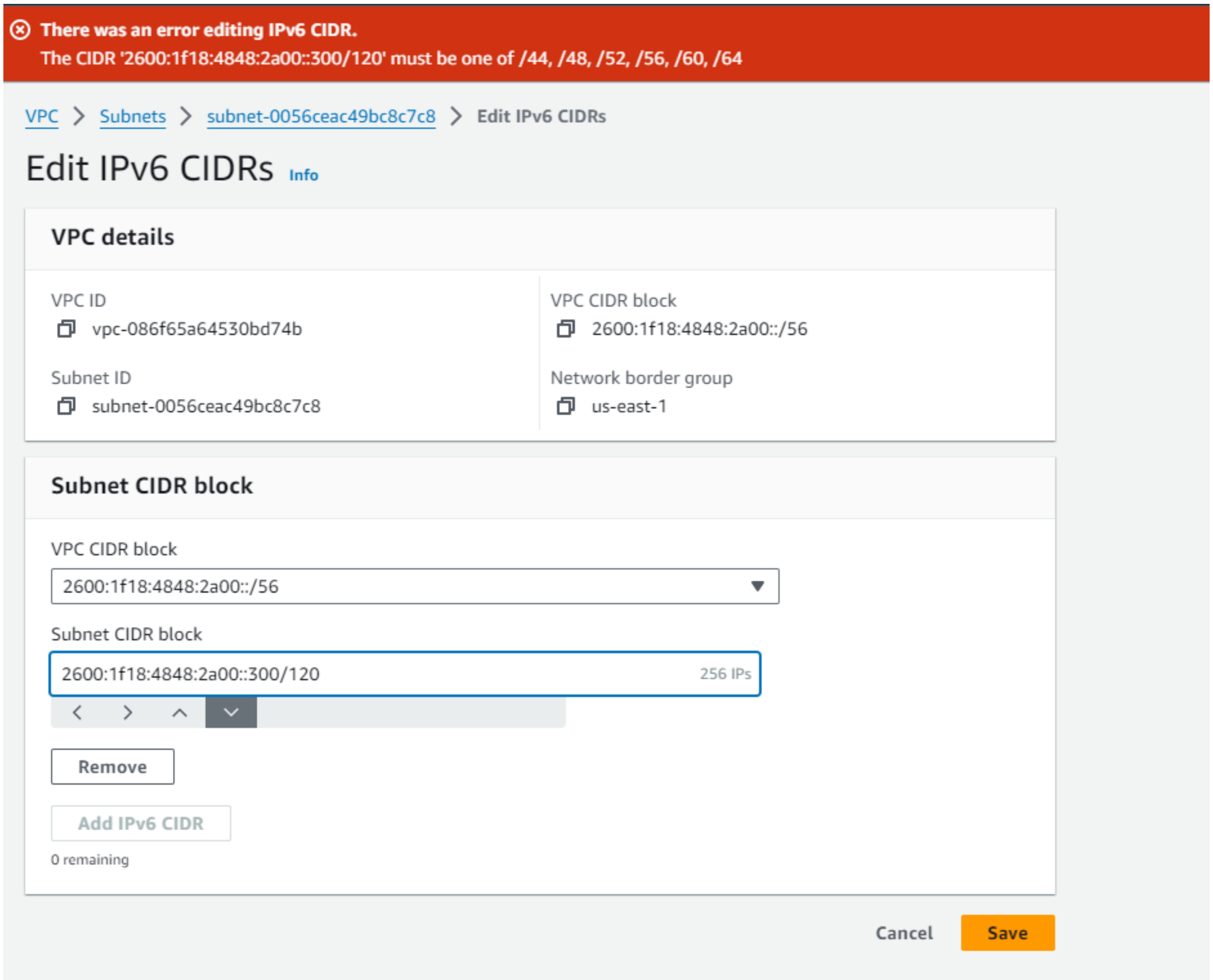


<u>**Section 2:**</u>

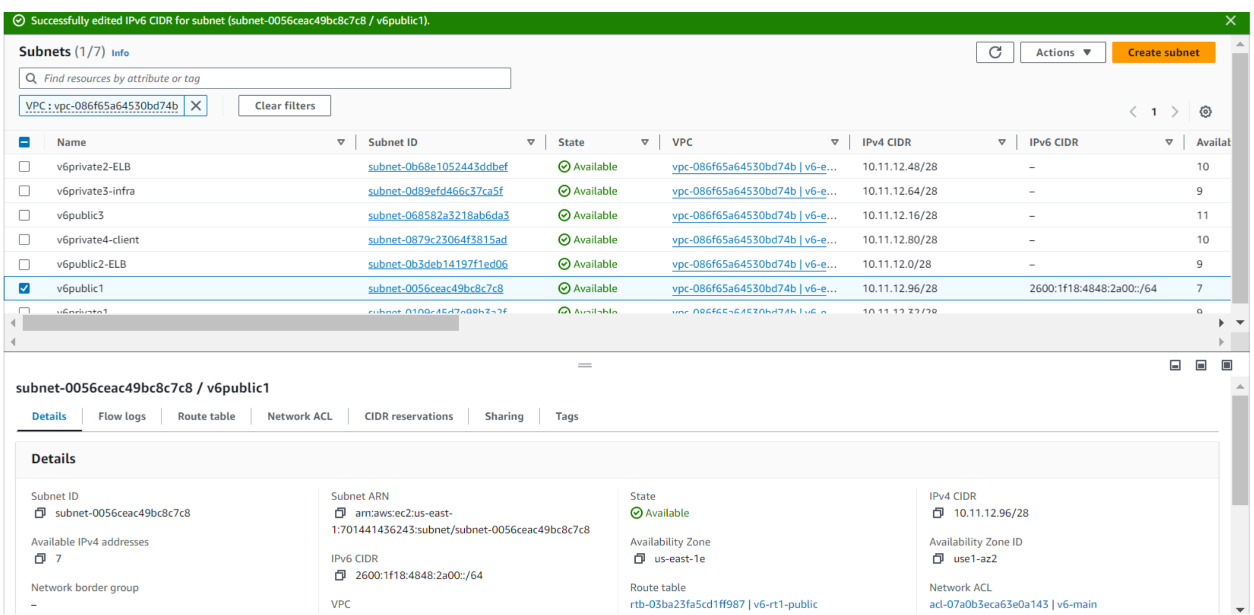
Now, let's enable IPv6 at each subnet level and observe the changes in the associated Security Groups and Instances within those specific subnets.



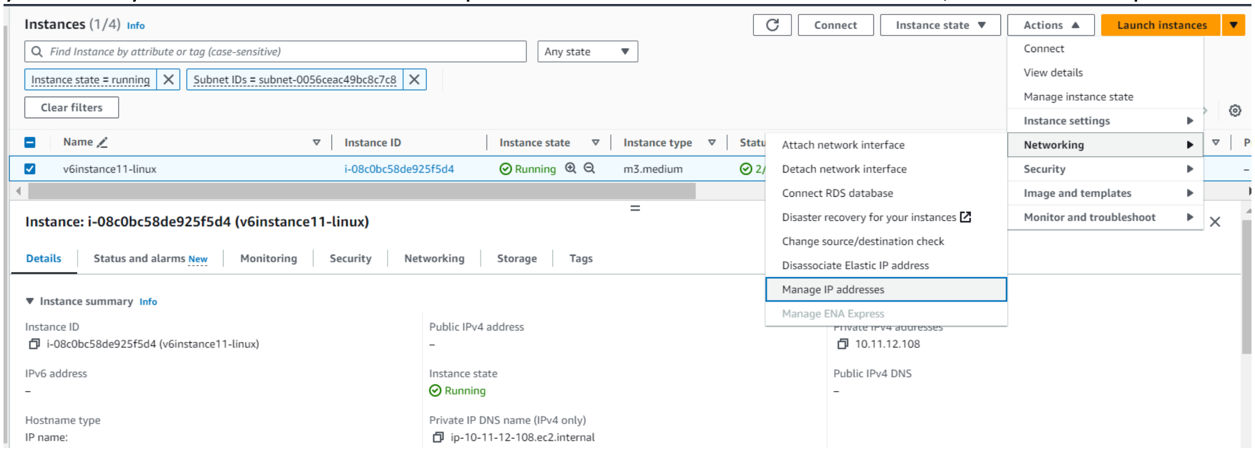


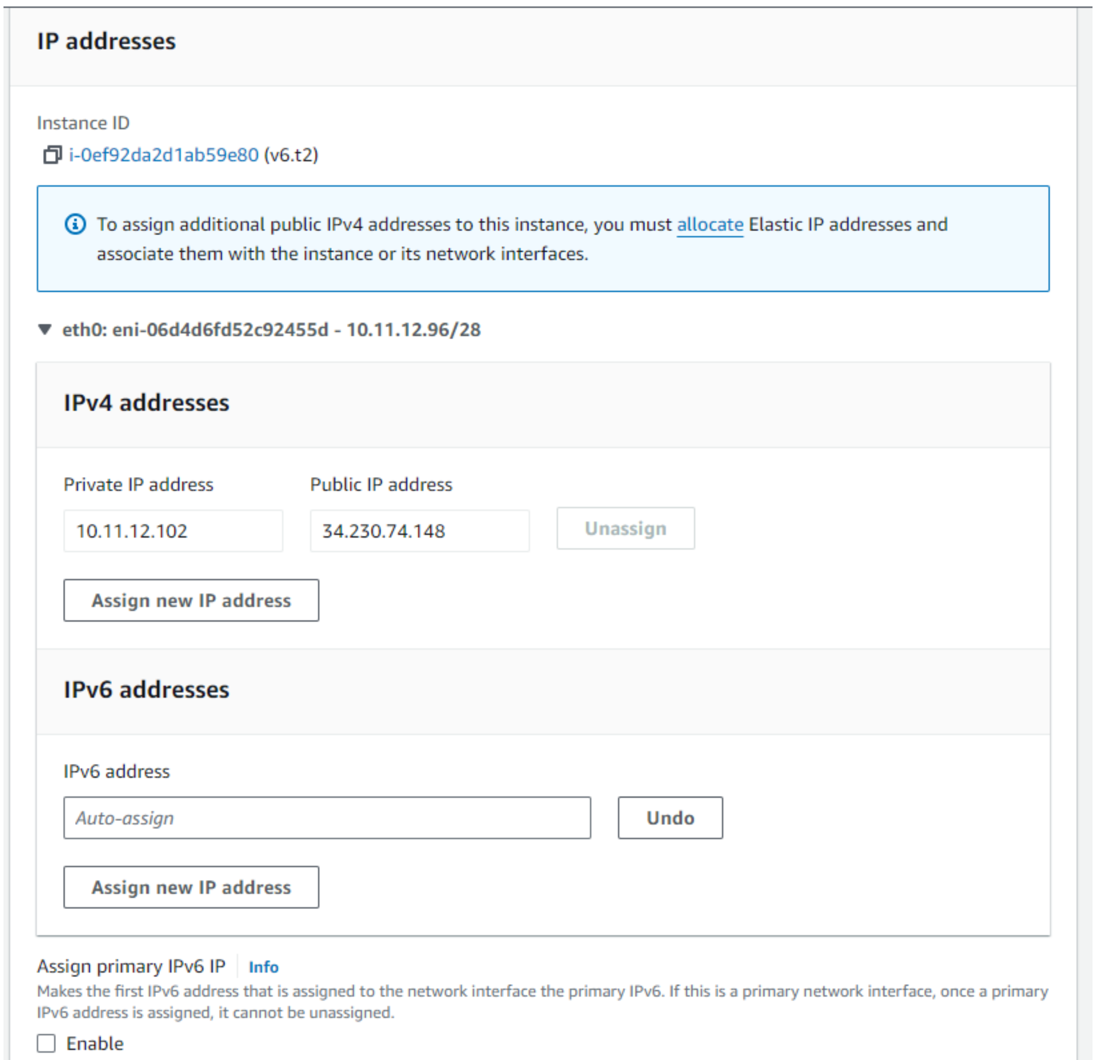


<u>Subnet with IPv6 having /64 CIDR</u>

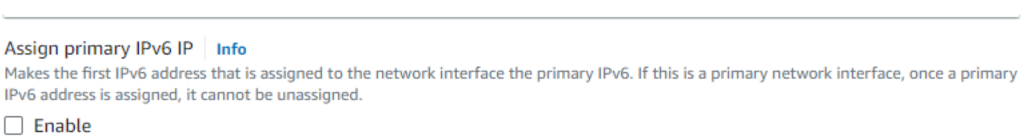


Enabling IPv6 on a subnet will not automatically assign IPv6 addresses to resources inside the subnet. If you want your EC2 instance in that specific subnet to have an IPv6 address, follow the steps below:





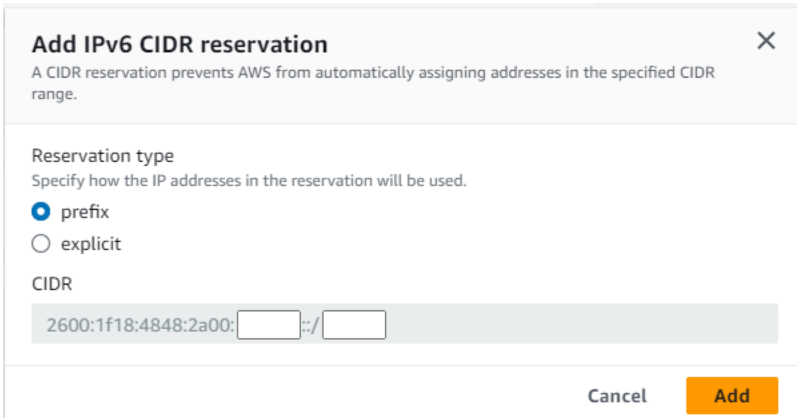
If you choose

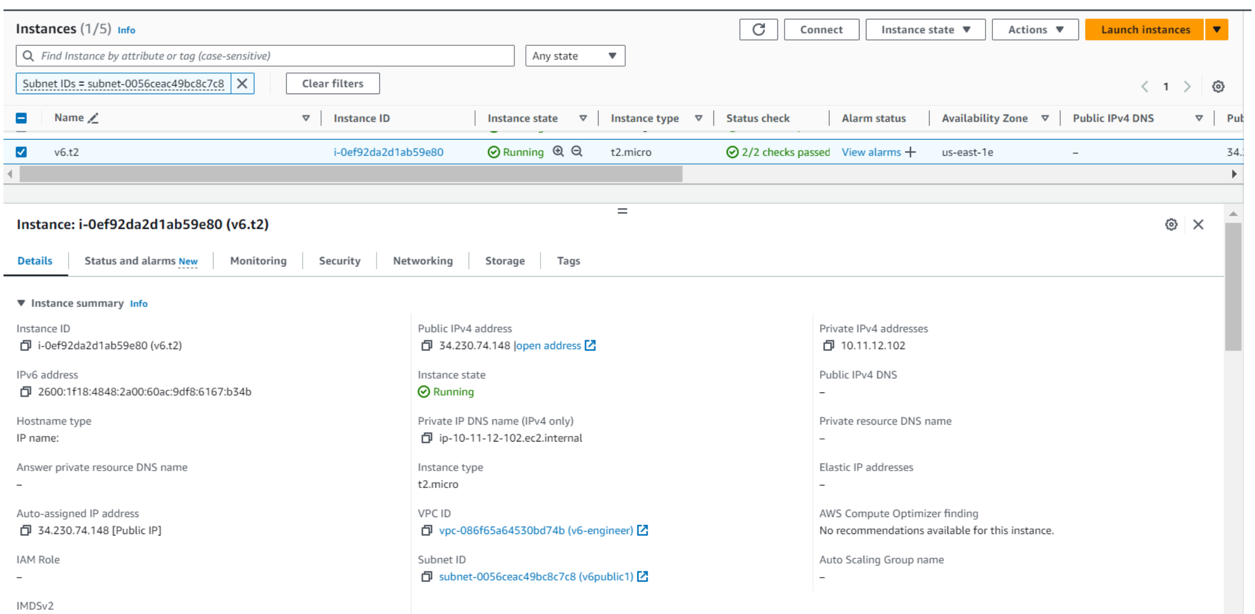


If you're modifying a network interface in a dual-stack or IPv6-only subnet, you have the option to Assign primary IPv6 IP. Enable a primary IPv6 address if you have instances or ENIs that rely on the IPv6 address not changing to avoid disrupting traffic to instances or ENIs.

When you enable an IPv6 GUA address to be a primary IPv6 address, you cannot disable it. Traffic will be routed to the primary IPv6 address until the instance is terminated or the ENI is detached.

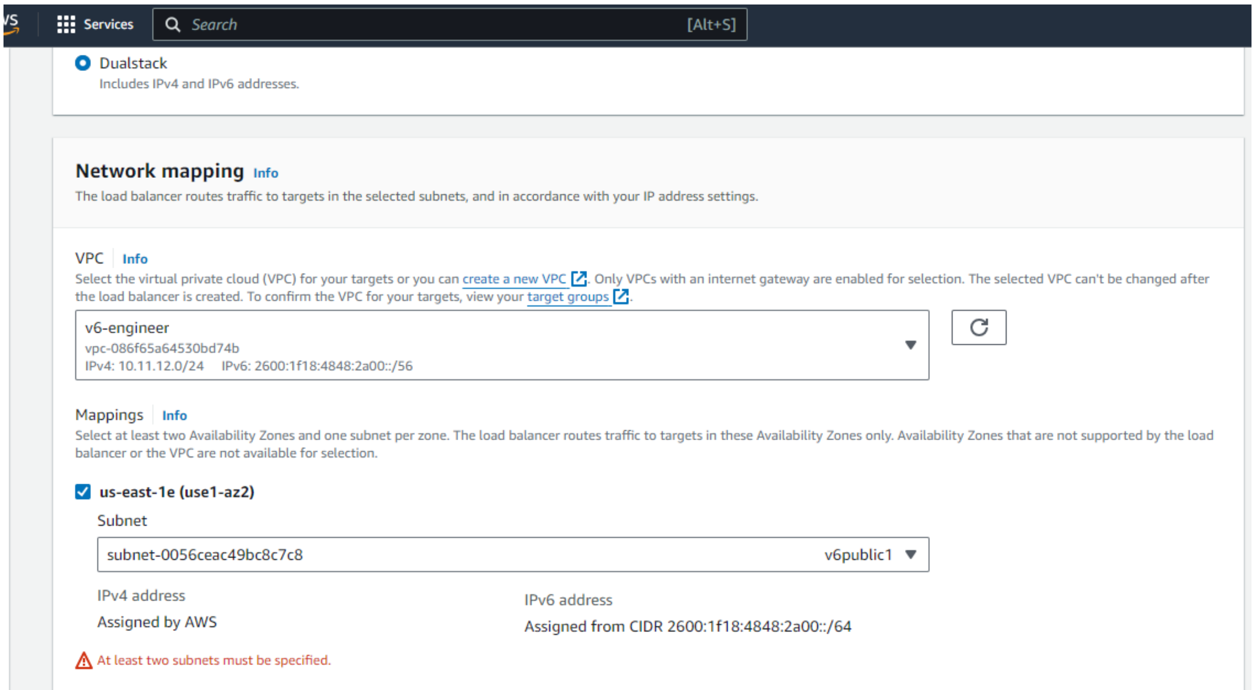
If you have multiple IPv6 addresses associated with an ENI and you enable a primary IPv6 address, the first IPv6 GUA address associated with the ENI becomes the primary IPv6 address.



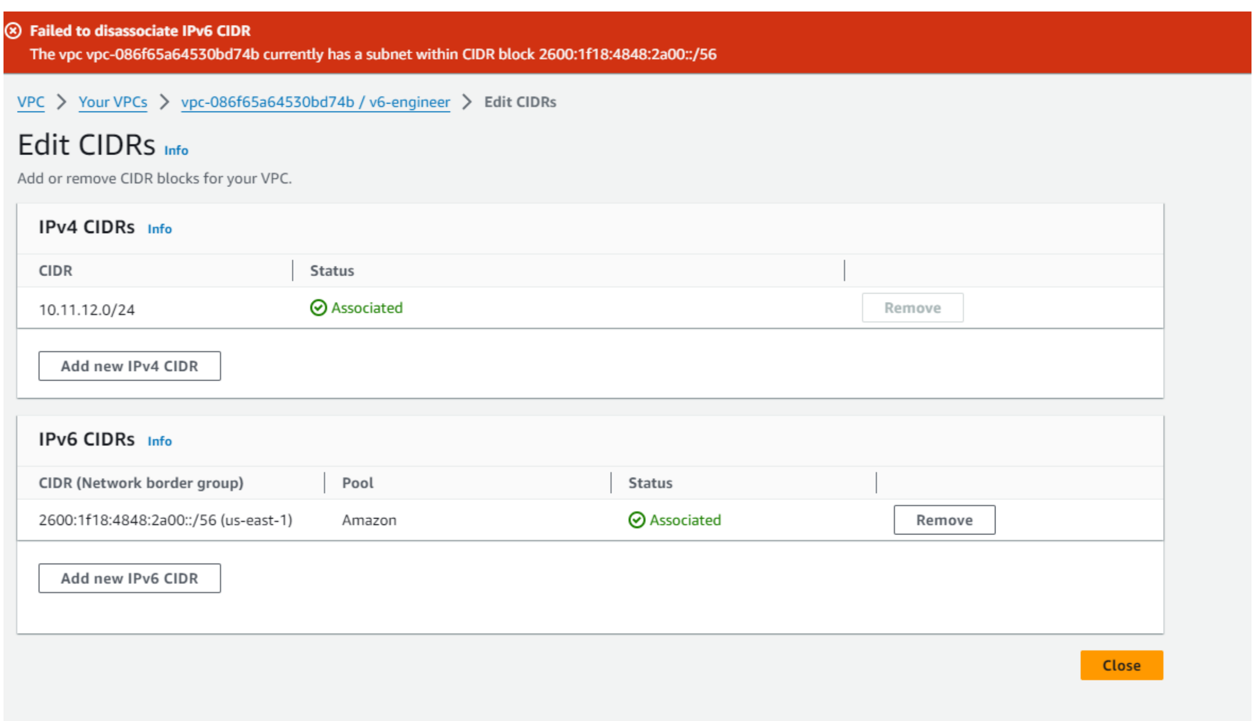


Just for the Information:

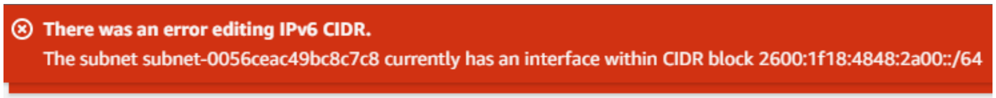
If, in the event that we are creating the load balancer within an existing IPv6 subnet, we will also observe the assigned IPv6 addresses for the load balancer.

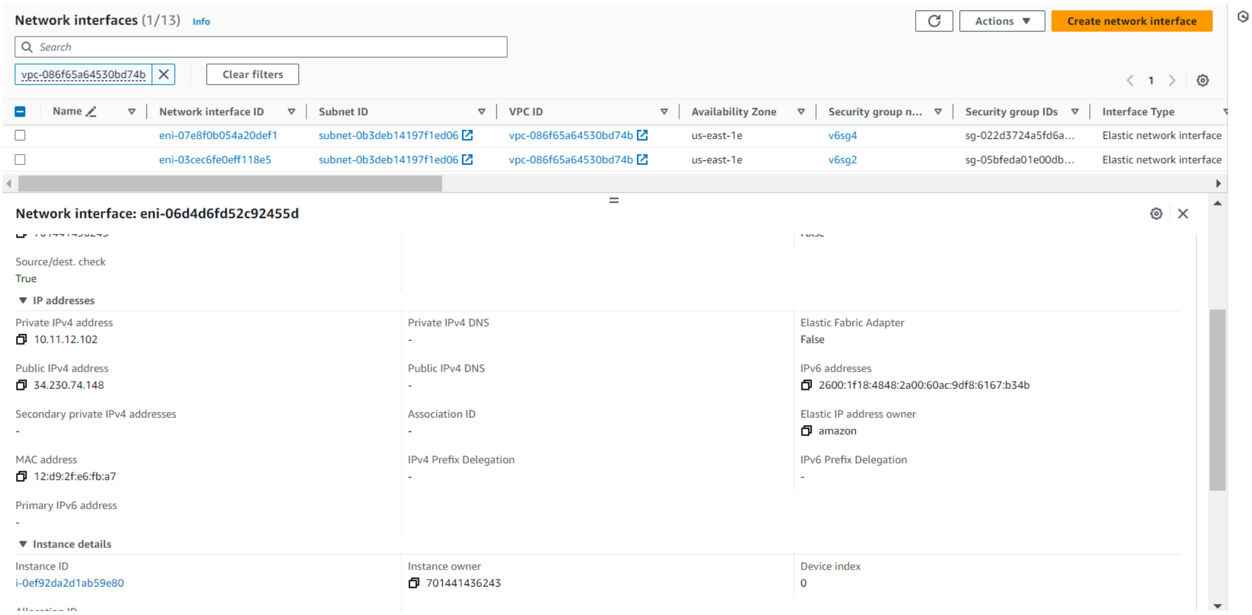


- If, in case, we attempt to remove IPv6 from the VPC level while IPv6 is still enabled on the subnet, an error will occur.

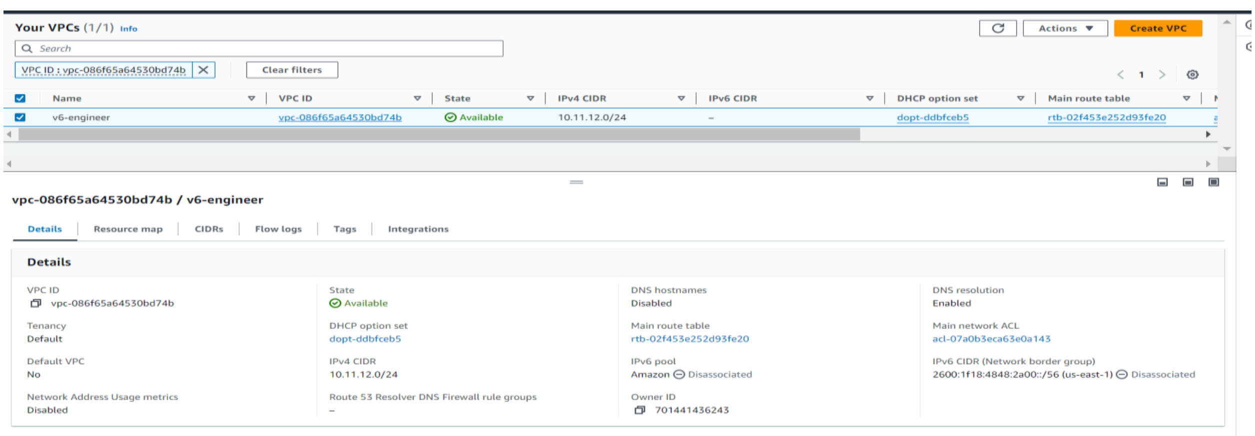


If you want to remove IPv6 on subnet directly:

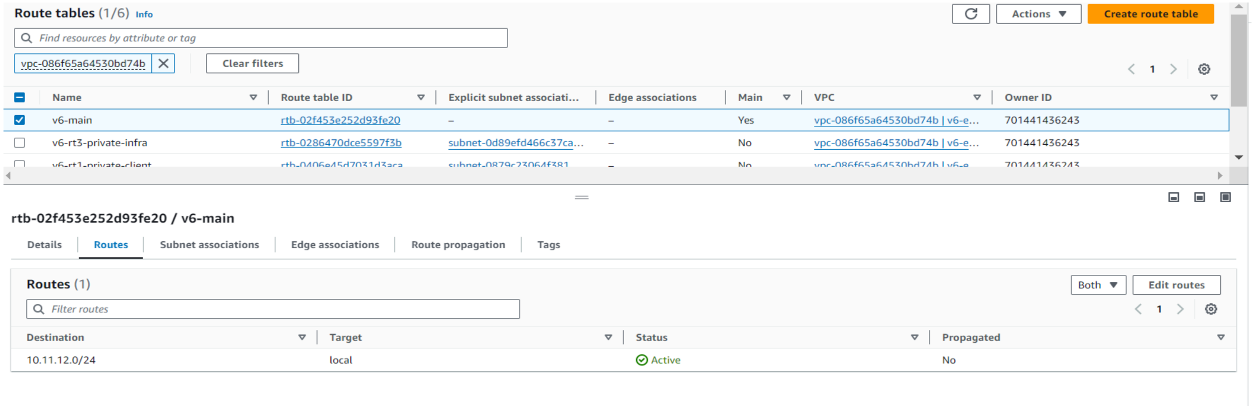




After detaching the ENI and removing IPv6 from subnet and VPC:



Main route table:



Route tables (1/6) Info

Filter: vpc-086f65a64530bd74b

Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC	Owner ID
v6-main	rtb-02f453e252d93fe20	–	–	Yes	vpc-086f65a64530bd74b | v6-e...	701441436243
v6-rt3-private-infra	rtb-0286470dce5597f3b	subnet-0d89efd466c37ca...	–	No	vpc-086f65a64530bd74b | v6-e...	701441436243

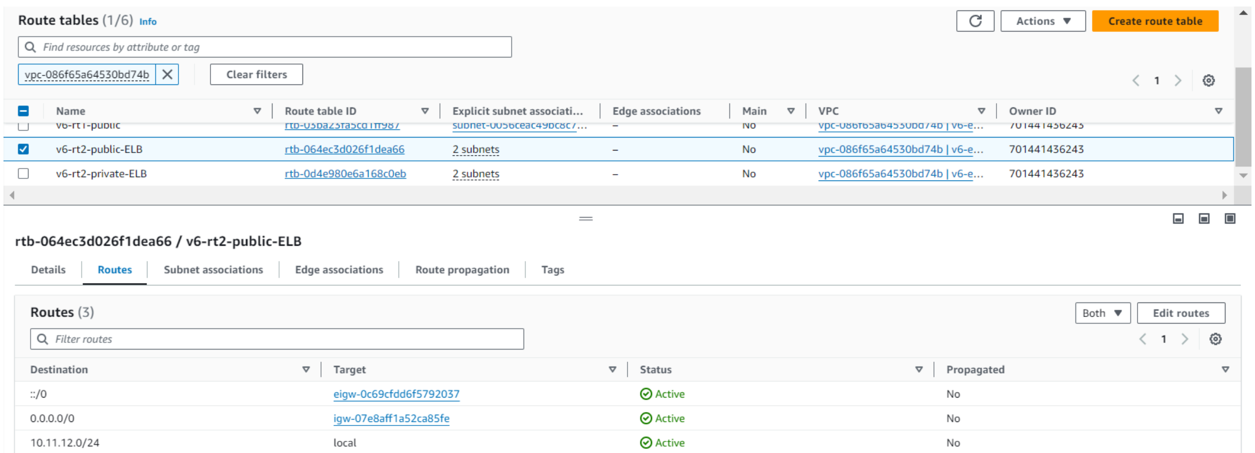
rtb-02f453e252d93fe20 / v6-main

Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

Destination	Target	Status	Propagated
10.11.12.0/24	local	Active	No

Custom route table:



Route tables (1/6) Info

Filter: vpc-086f65a64530bd74b

Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC	Owner ID
v6-rt2-public-ELB	rtb-064ec3d026f1dea66	2 subnets	–	No	vpc-086f65a64530bd74b | v6-e...	701441436243
v6-rt2-private-ELB	rtb-0d4e980e6a168c0eb	2 subnets	–	No	vpc-086f65a64530bd74b | v6-e...	701441436243

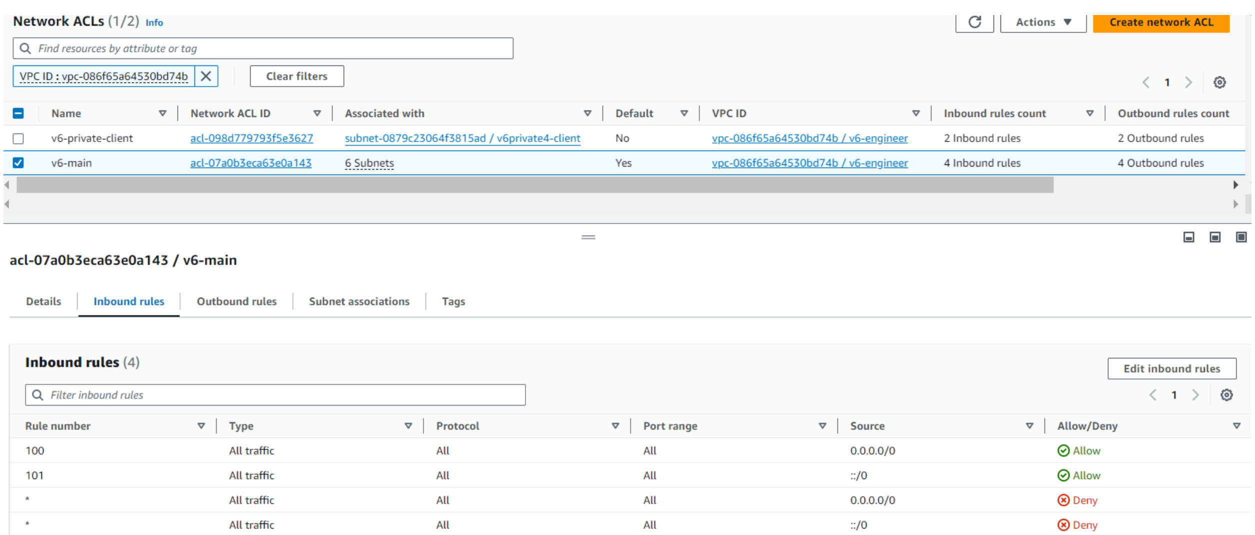
rtb-064ec3d026f1dea66 / v6-rt2-public-ELB

Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (3)

Destination	Target	Status	Propagated
::/0	eigw-0c69cfdd6f5792037	Active	No
0.0.0.0/0	igw-07e8aff1a52ca85fe	Active	No
10.11.12.0/24	local	Active	No

Main NACL:



Network ACLs (1/2) Info

Filter: VPC ID : vpc-086f65a64530bd74b

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
v6-private-client	acl-098d779793f5e3627	subnet-0879c23064f3815ad / v6private4-client	No	vpc-086f65a64530bd74b / v6-engineer	2 Inbound rules	2 Outbound rules
v6-main	acl-07a0b3eca63e0a143	6 Subnets	Yes	vpc-086f65a64530bd74b / v6-engineer	4 Inbound rules	4 Outbound rules

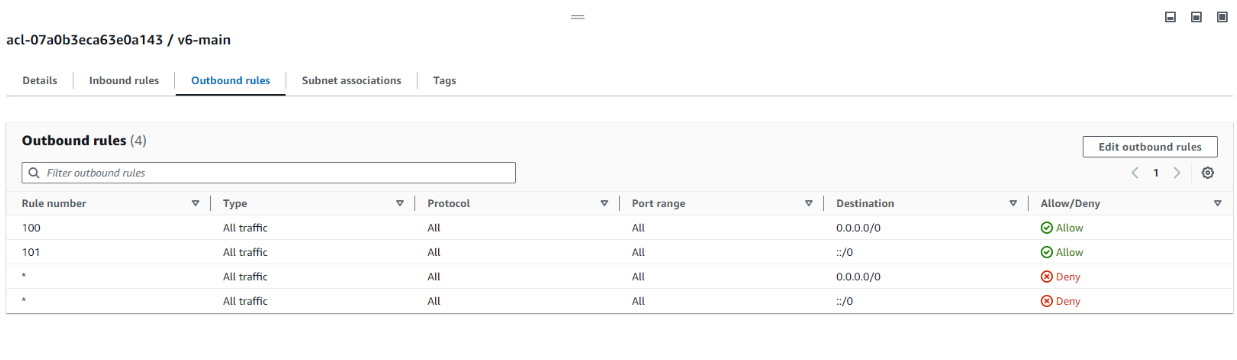
acl-07a0b3eca63e0a143 / v6-main

Details | Inbound rules | Outbound rules | Subnet associations | Tags

Inbound rules (4)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	All traffic	All	All	::/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

Outbound:



acl-07a0b3eca63e0a143 / v6-main

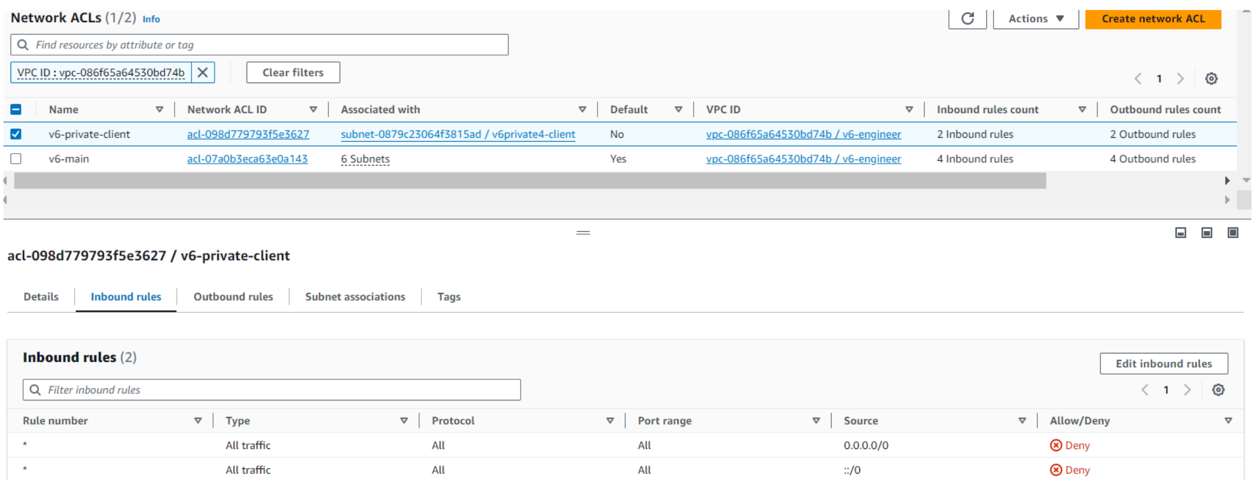
Details | Inbound rules | Outbound rules | Subnet associations | Tags

Outbound rules (4)

Edit outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
101	All traffic	All	All	::/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

Custom NACL inbound:



Network ACLs (1/2) Info

Actions | Create network ACL

VPC ID : vpc-086f65a64530bd74b | Clear filters

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
v6-private-client	acl-098d779793f5e3627	subnet-0879c23064f3815ad / v6private4-client	No	vpc-086f65a64530bd74b / v6-engineer	2 Inbound rules	2 Outbound rules
v6-main	acl-07a0b3eca63e0a143	6 Subnets	Yes	vpc-086f65a64530bd74b / v6-engineer	4 Inbound rules	4 Outbound rules

acl-098d779793f5e3627 / v6-private-client

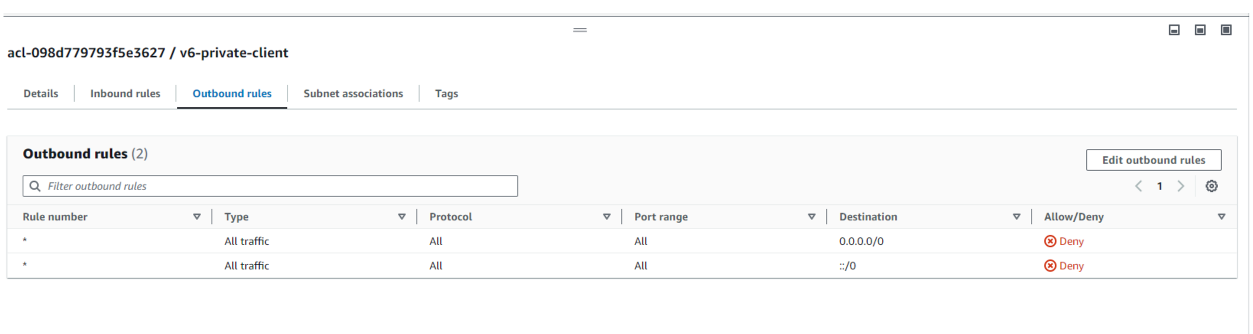
Details | Inbound rules | Outbound rules | Subnet associations | Tags

Inbound rules (2)

Edit inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

Custom NACL outbound:



acl-098d779793f5e3627 / v6-private-client

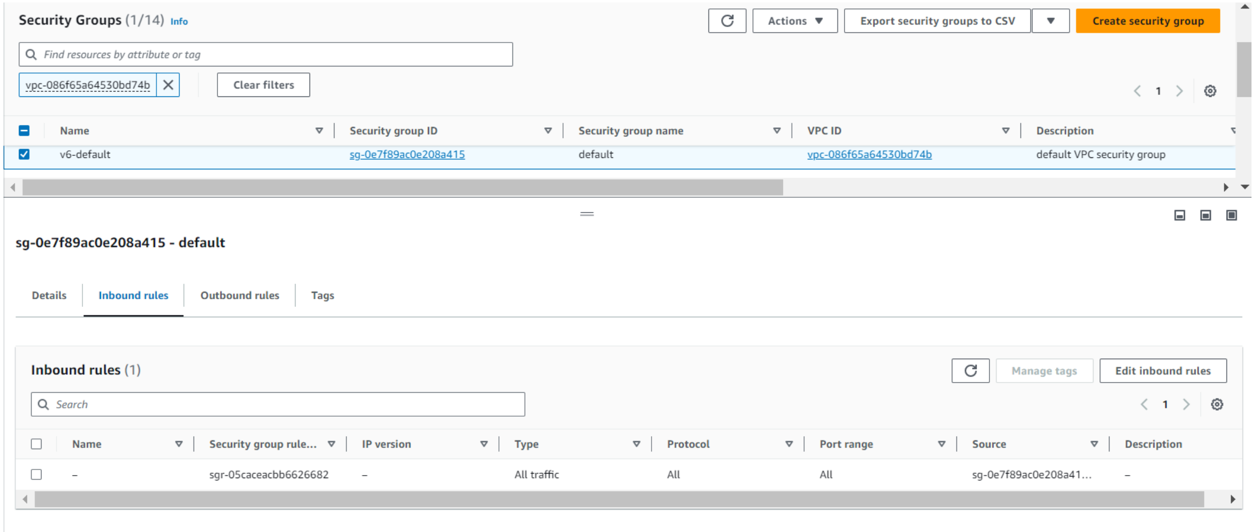
Details | Inbound rules | Outbound rules | Subnet associations | Tags

Outbound rules (2)

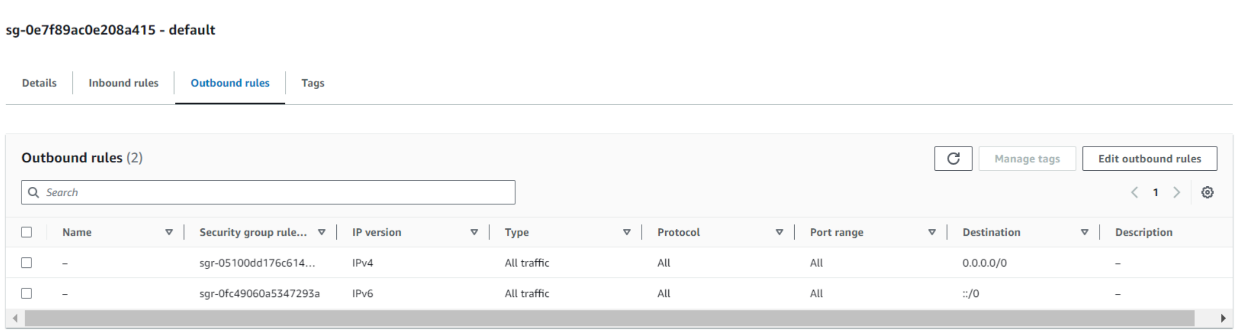
Edit outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny
*	All traffic	All	All	::/0	Deny

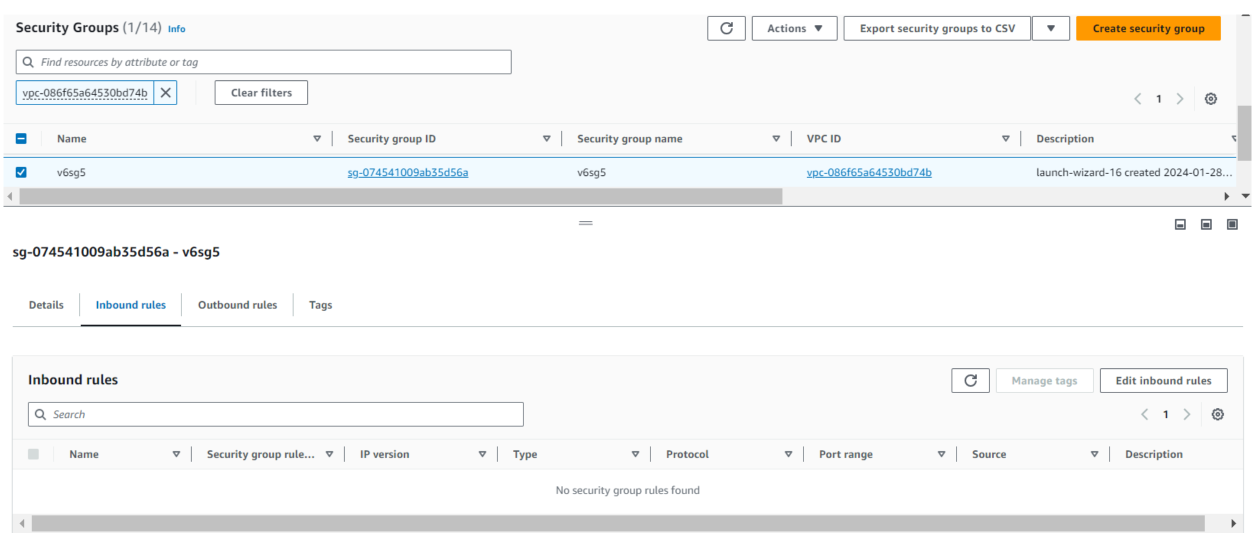
Default security group inbound:



Default security group outbound:



Instance default security group inbound:



Instance default security group outbound: