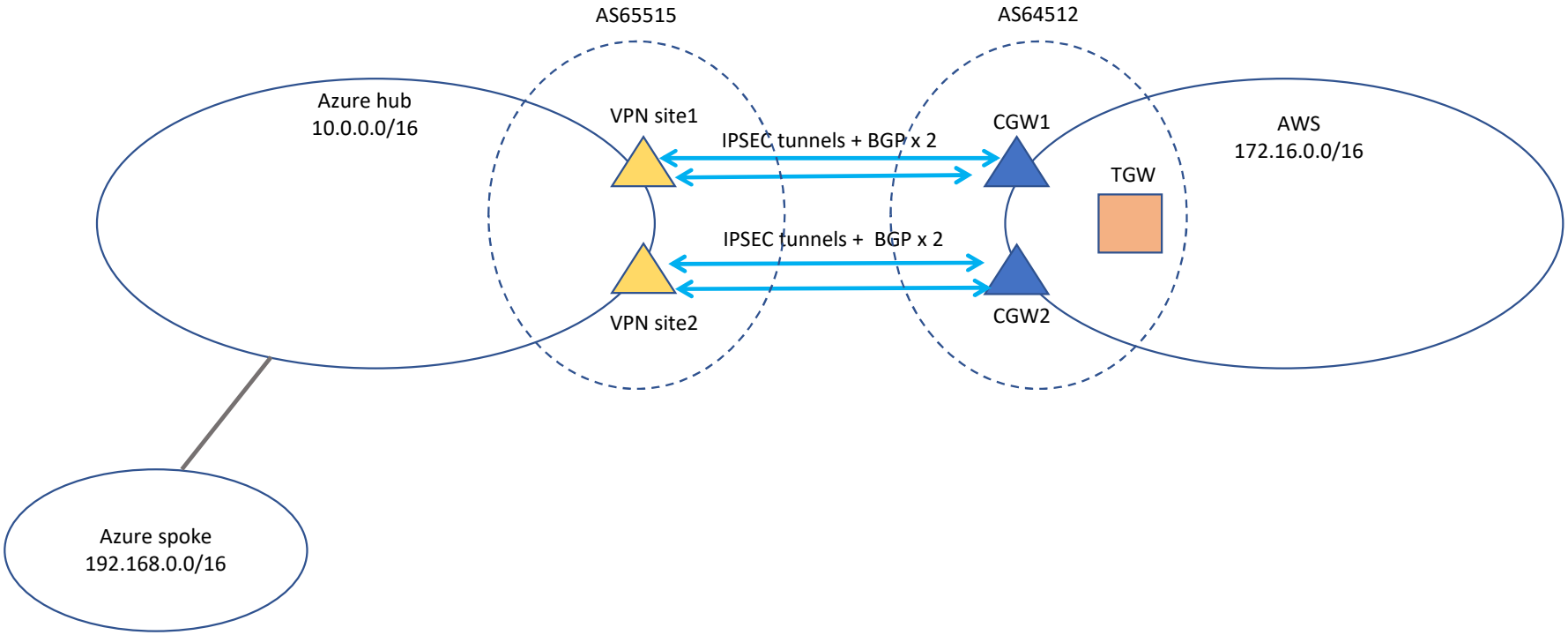
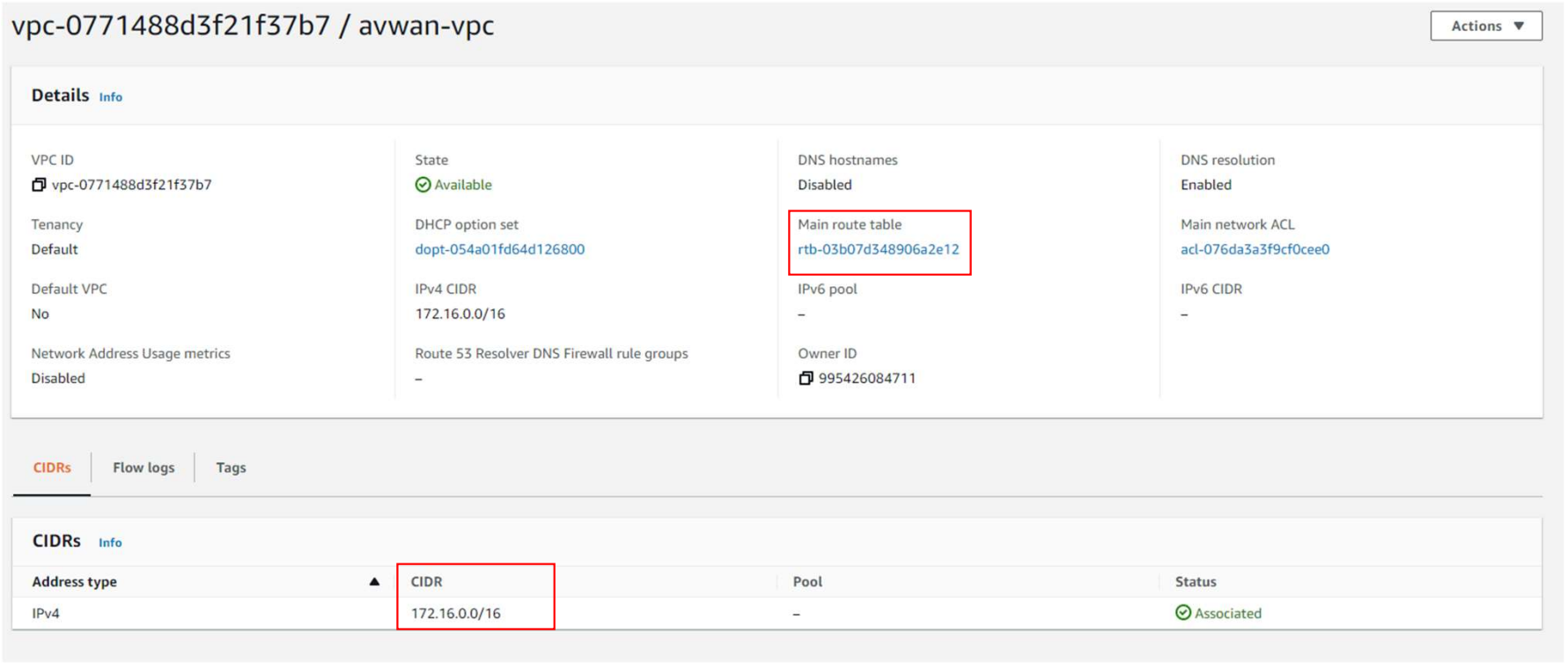
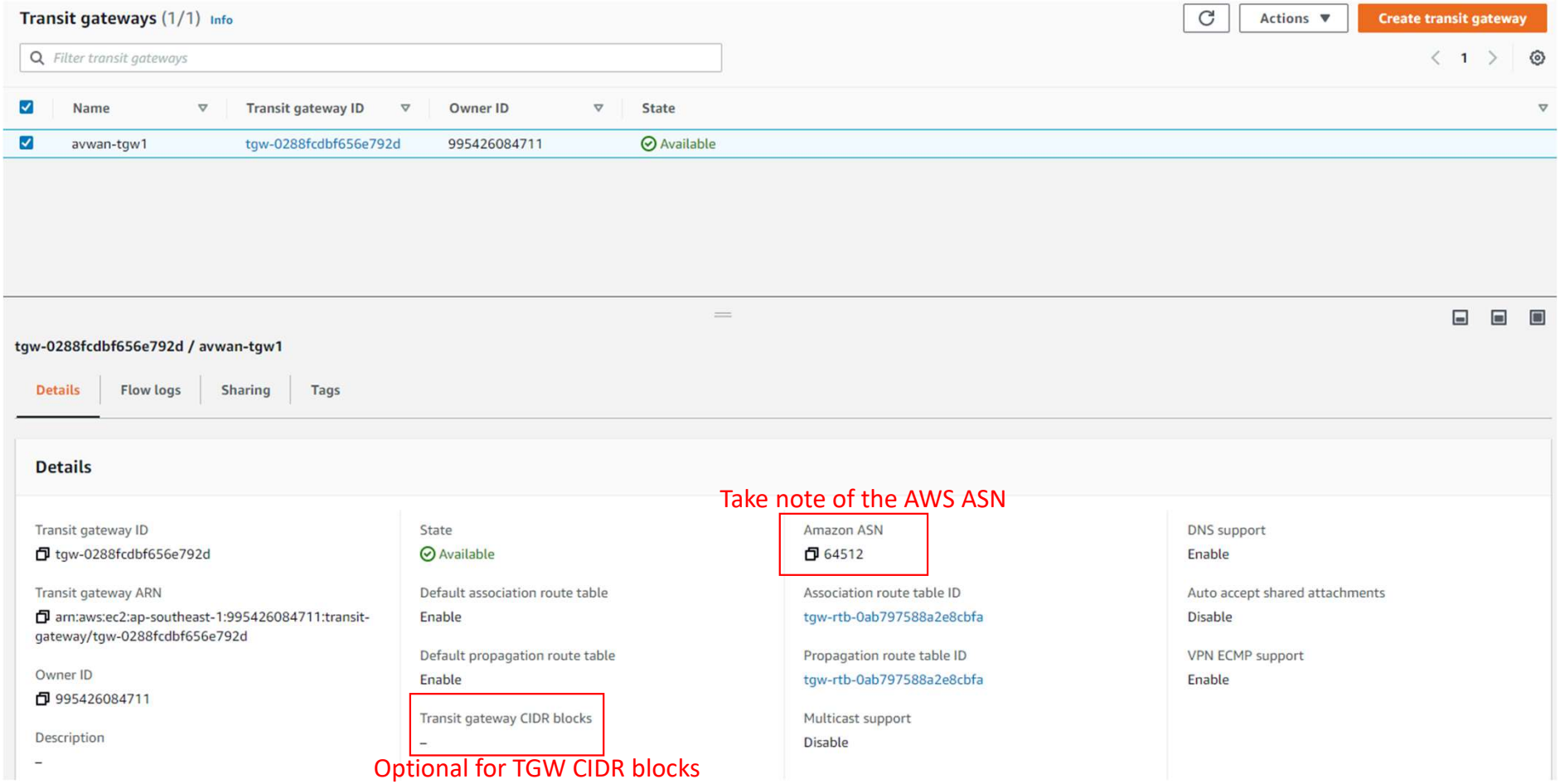
S2S VPN between Azure VWAN Hub and AWS TGW



AWS configuration – VPC setup

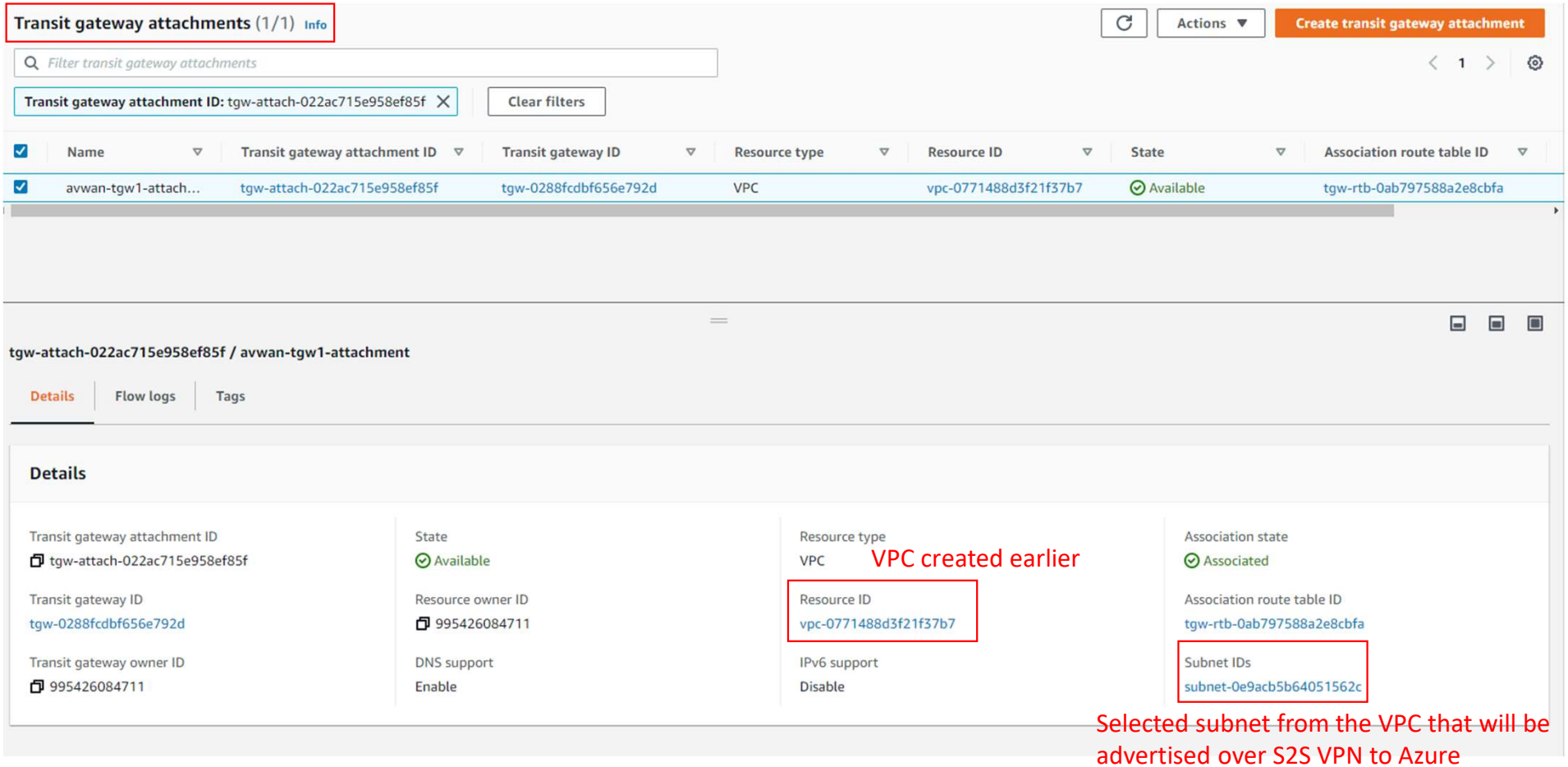


AWS configuration – TGW



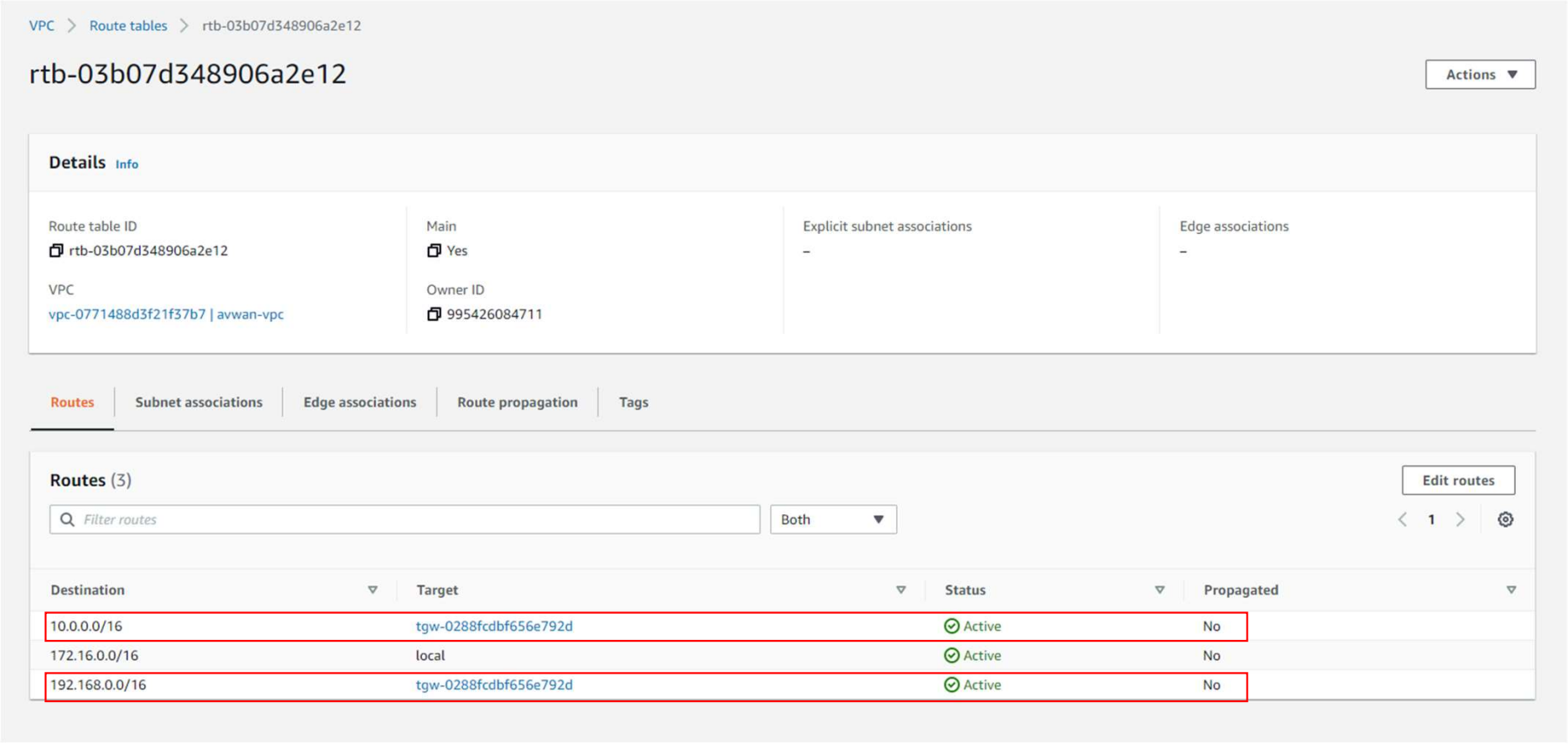
AWS configuration – TGW attachment to VPC

Here you need to create TGW attachment to attach the TGW to the VPC



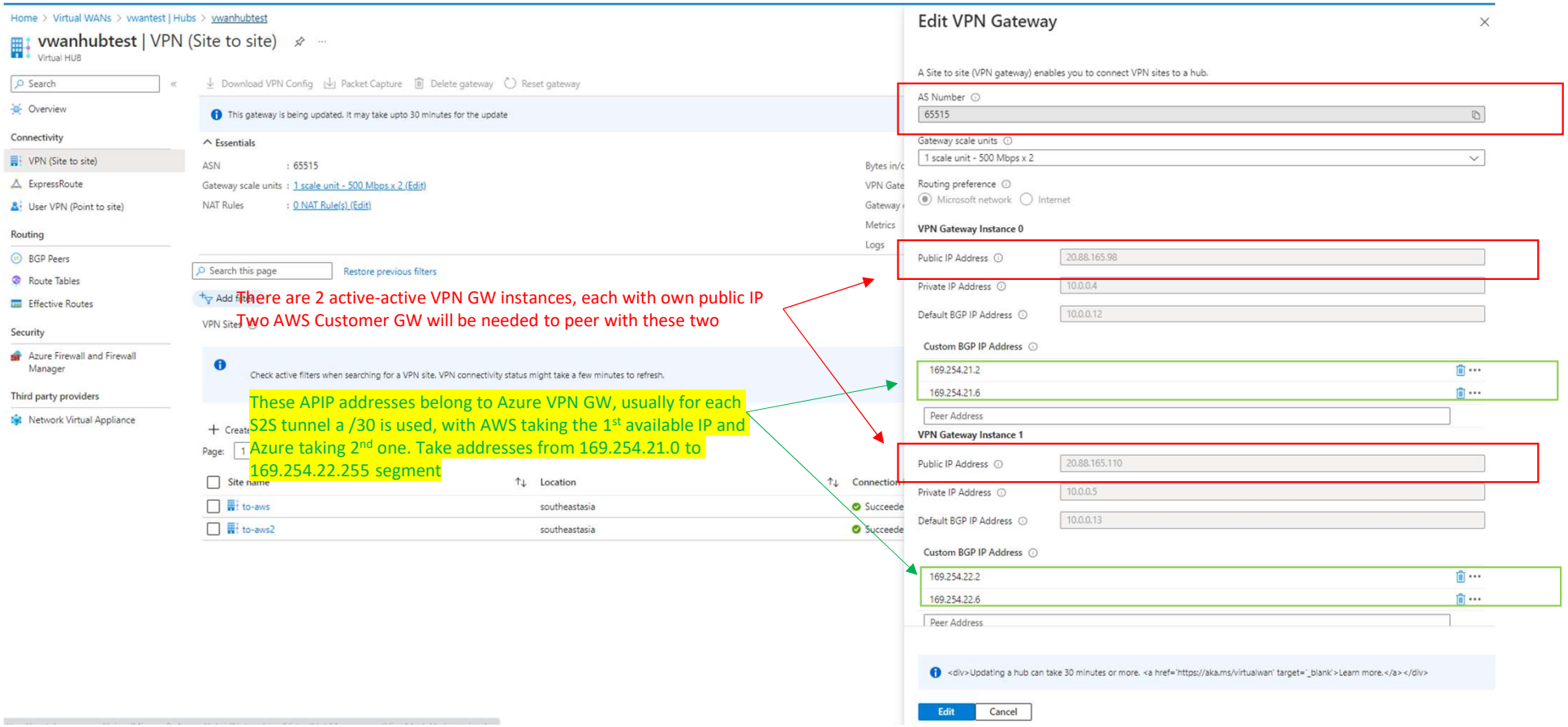
AWS configuration – Modify VPC route table to route Azure subnets to TGW

On the VPC route table, route the Azure subnets of 10.0.0.0/16 and 192.168.0.0/16 to the TGW. This is done manually. TGW will learn of these prefixes via BGP later. This step is needed as VPC route table ≠ TGW route table



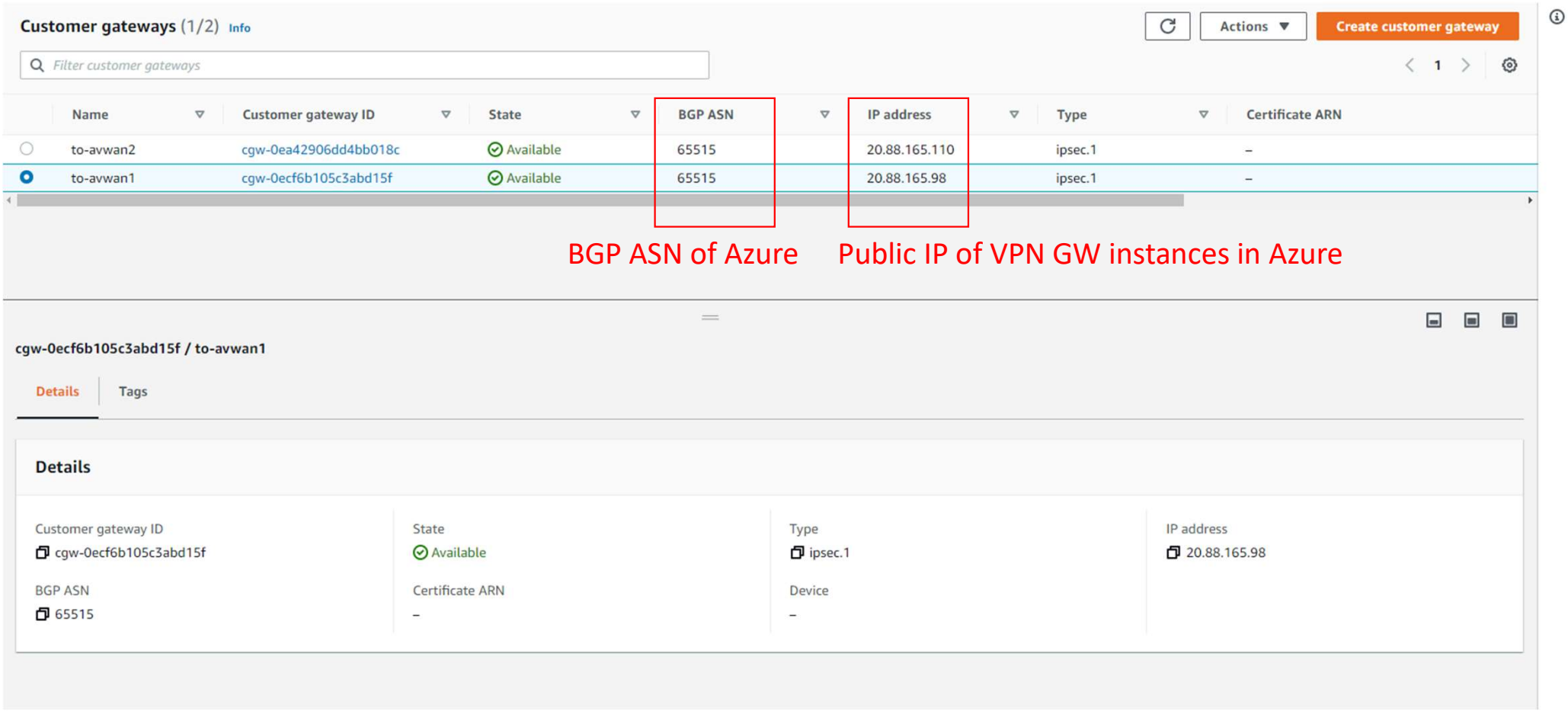
Azure configuration – Create new VPN Gateway under VWAN Hub

Assume VWAN and VWAN Hub are setup, create VPN gateway under VWAN Hub. Note the ASN and public IP of the Gateway Instance. Also provide APIP addresses in the range 169.254.21.0 to 169.254.22.255



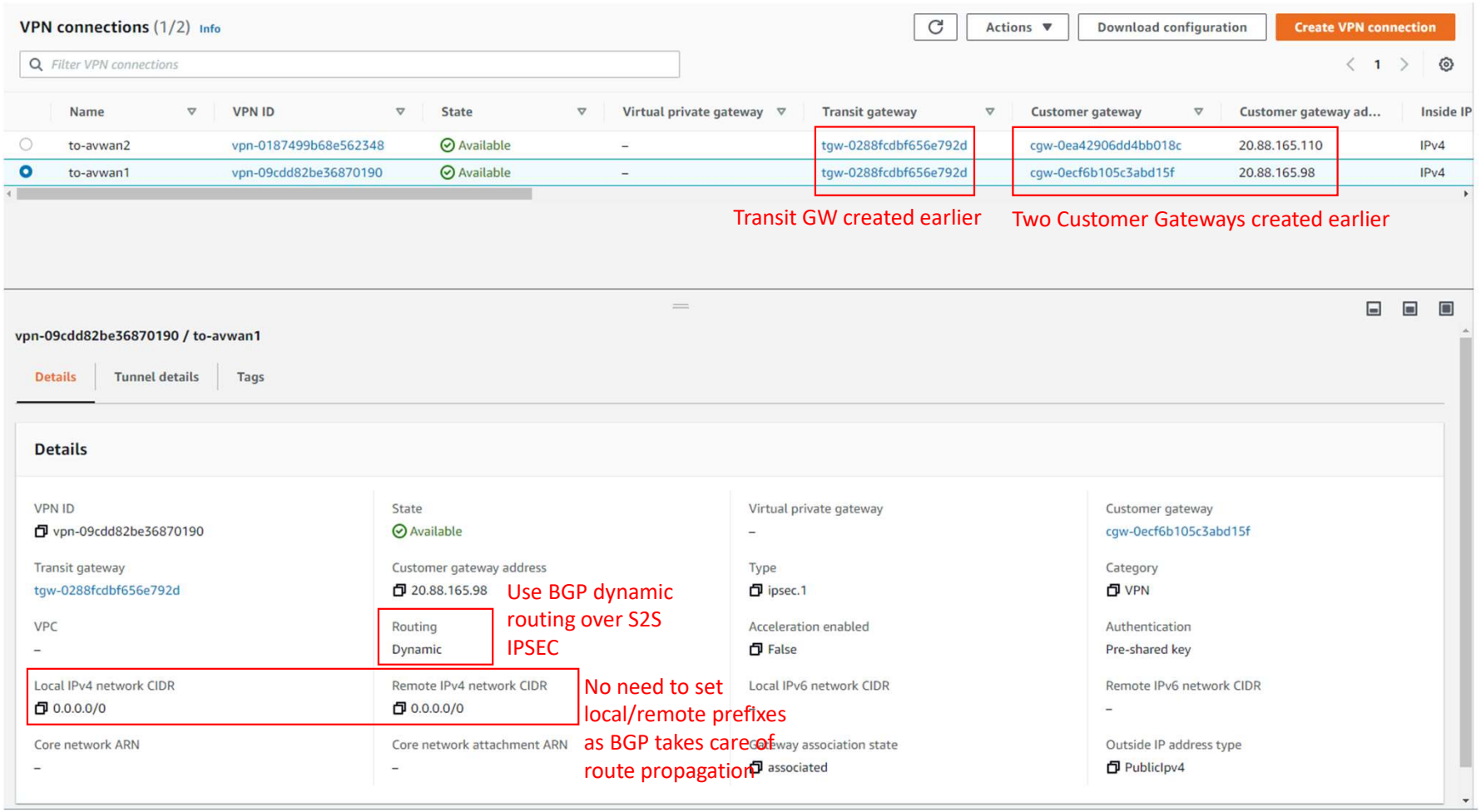
AWS configuration – Create two Customer Gateways each representing the VPN GW instances on Azure

Assume VWAN and VWAN Hub are setup, create VPN gateway under VWAN Hub. Note the ASN and public IP of the Gateway Instance. Also provide APIP addresses in the range 169.254.21.0 to 169.254.22.255



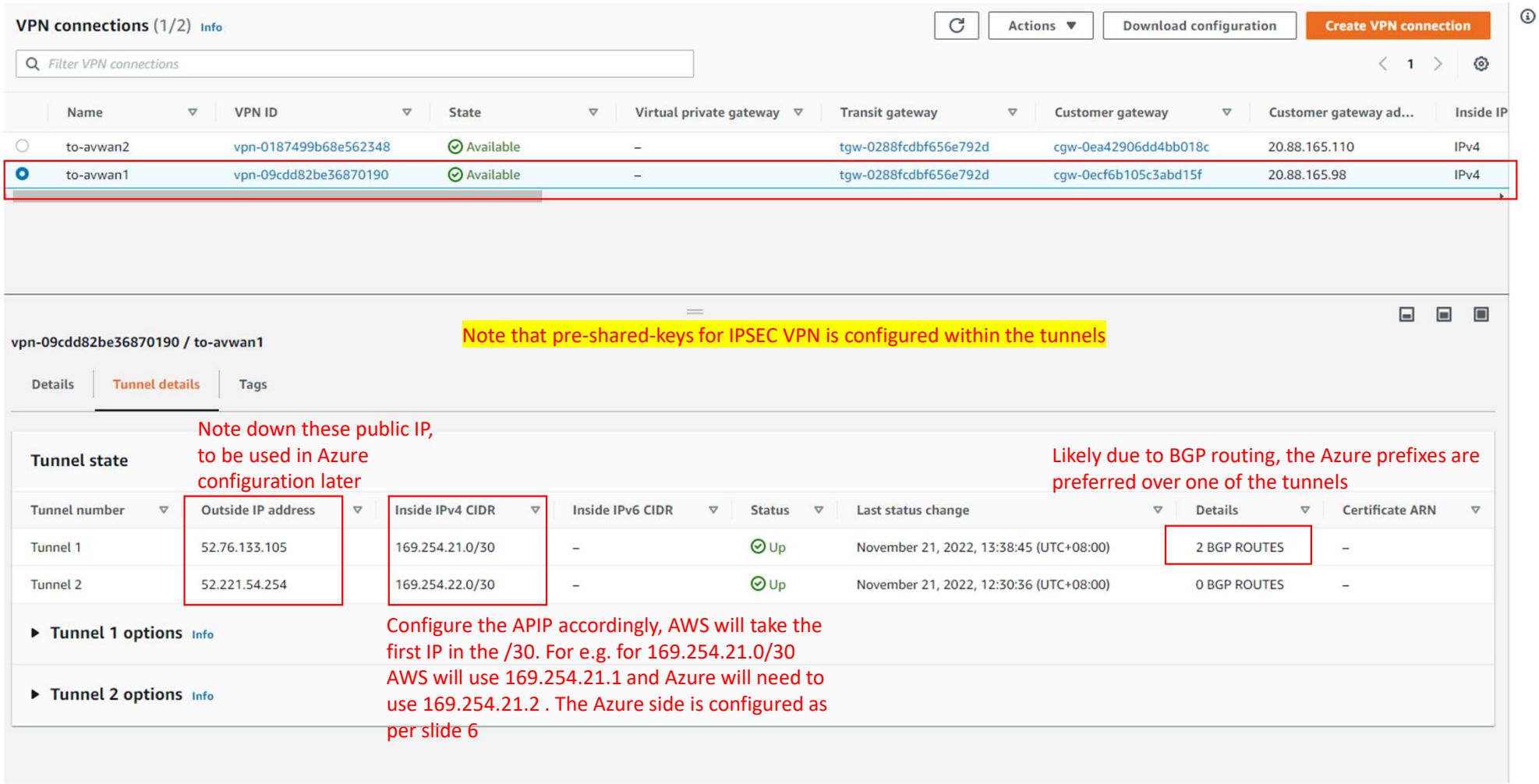
AWS configuration – Create S2S VPN using the CGW and TGW

Assume VWAN and VWAN Hub are setup, create VPN gateway under VWAN Hub. Note the ASN and public IP of the Gateway Instance. Also provide APIP addresses in the range 169.254.21.0 to 169.254.22.255



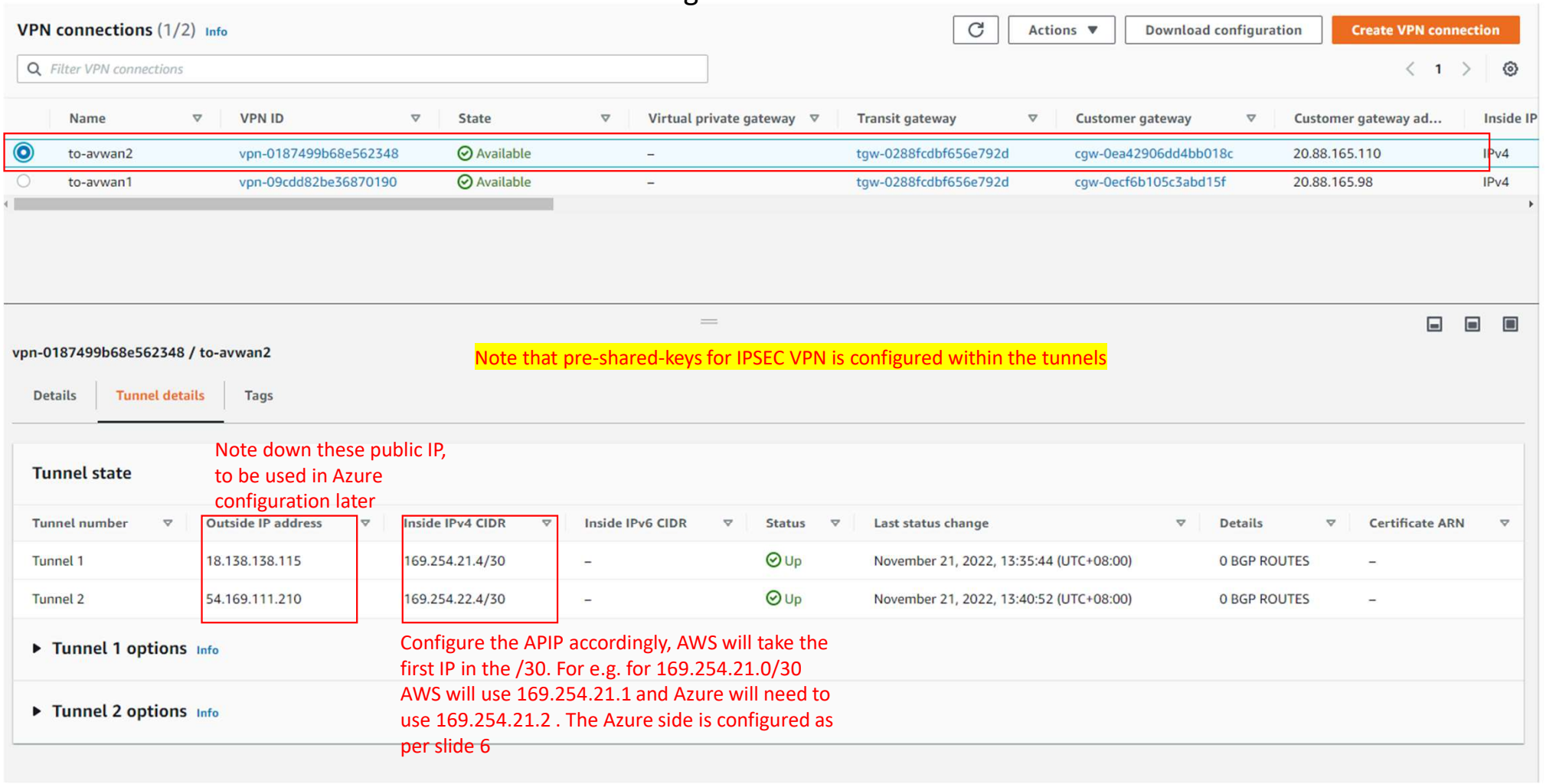
AWS configuration – Create S2S VPN using the CGW and TGW

Each S2S VPN has 2 tunnels – enter the details using the correct APIP addresses



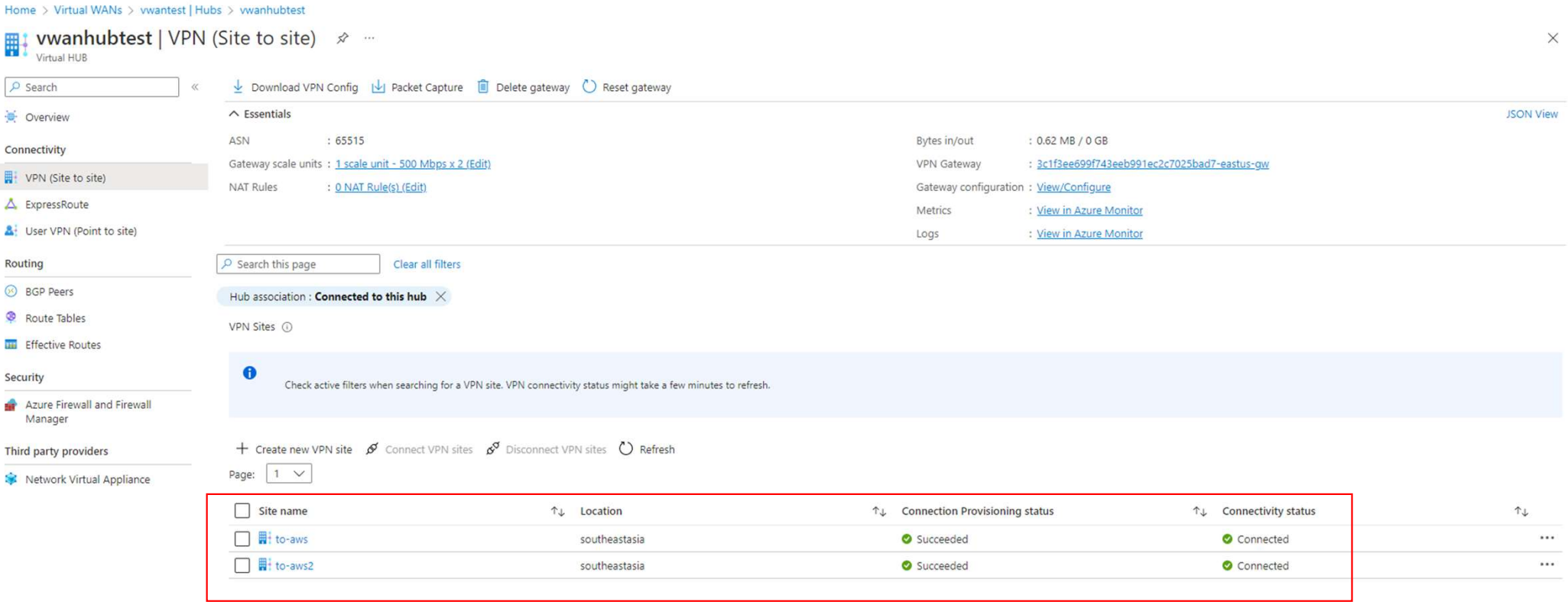
AWS configuration – Create S2S VPN using the CGW and TGW

Each S2S VPN has 2 tunnels – enter the details using the correct APIP addresses



Azure S2S VPN configuration under VPN GW of VWAN Hub

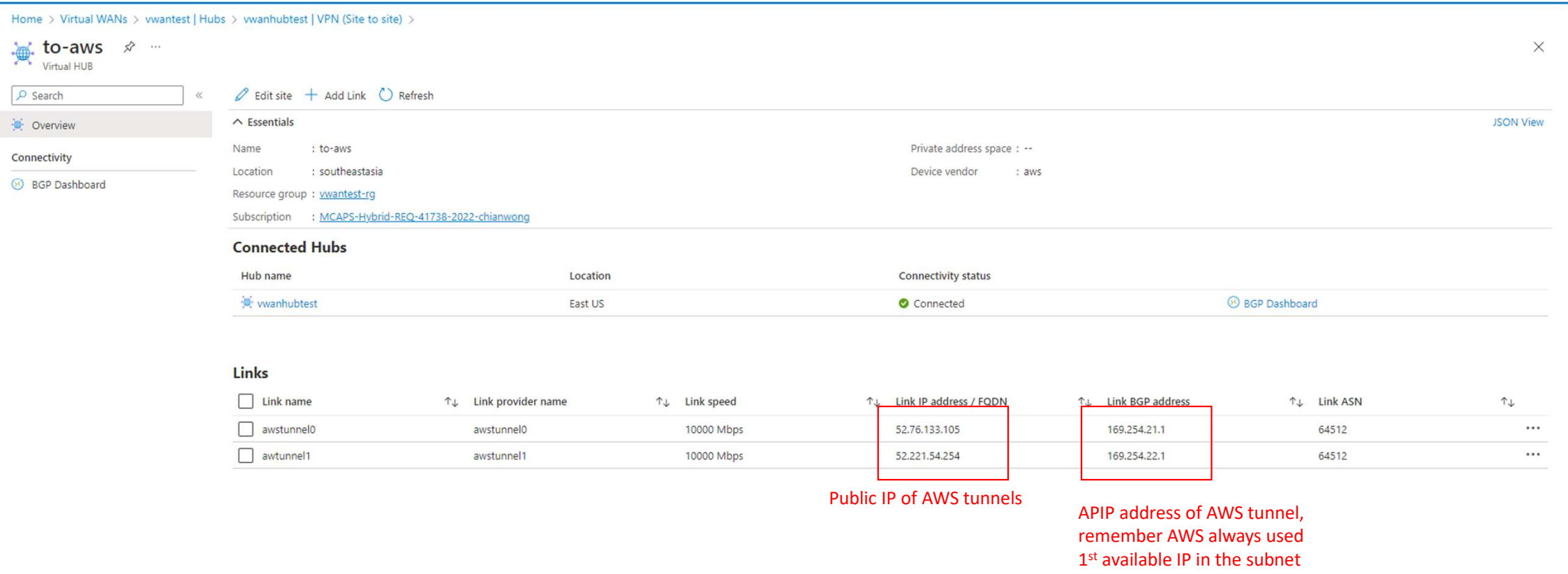
Here 2 S2S VPN objects are used, each with 2 tunnels. You can also choose to use 1 S2S VPN object with 4 tunnels



Two VPN “site” objects created each with 2 tunnels, you can also use 1 VPN site object with 4 tunnels

Azure S2S VPN configuration under VPN GW of VWAN Hub

Tunnel configuration for one of the VPN objects

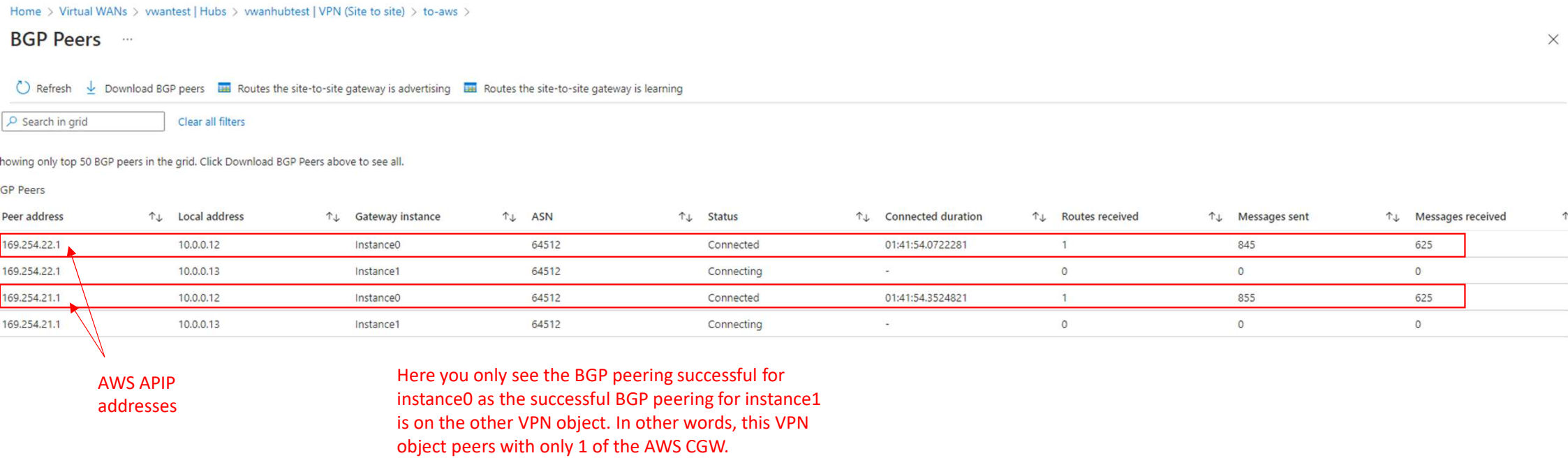


Public IP of AWS tunnels

APIP address of AWS tunnel, remember AWS always used 1st available IP in the subnet

Azure S2S VPN configuration under VPN GW of VWAN Hub

BGP peering status for one of the VPN objects

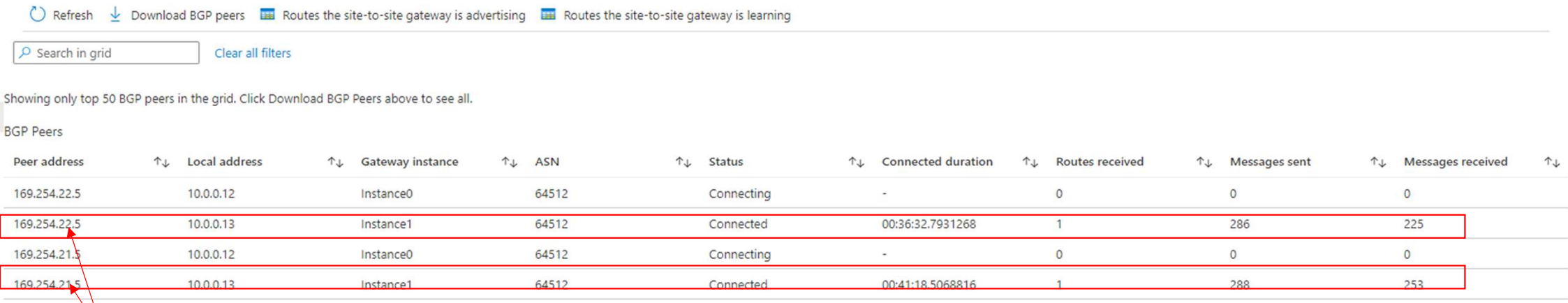


AWS APIP addresses

Here you only see the BGP peering successful for instance0 as the successful BGP peering for instance1 is on the other VPN object. In other words, this VPN object peers with only 1 of the AWS CGW.

Azure S2S VPN configuration under VPN GW of VWAN Hub

BGP peering status the other VPN object

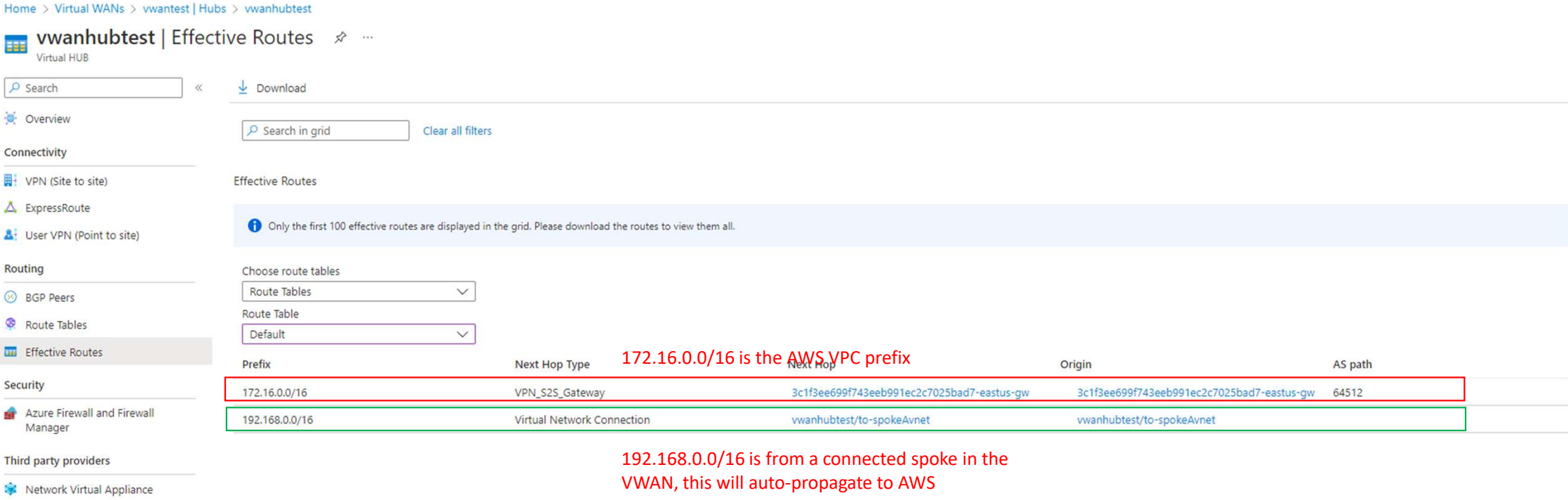


AWS APIP addresses

Here you only see the BGP peering successful for instance1 as the successful BGP peering for instance0 is on the other VPN object. In other words, this VPN object peers with only 1 of the AWS CGW.

Azure Route Table on VWAN hub

The 172.16.0.0/16 AWS prefix is received via S2S VPN as confirmed

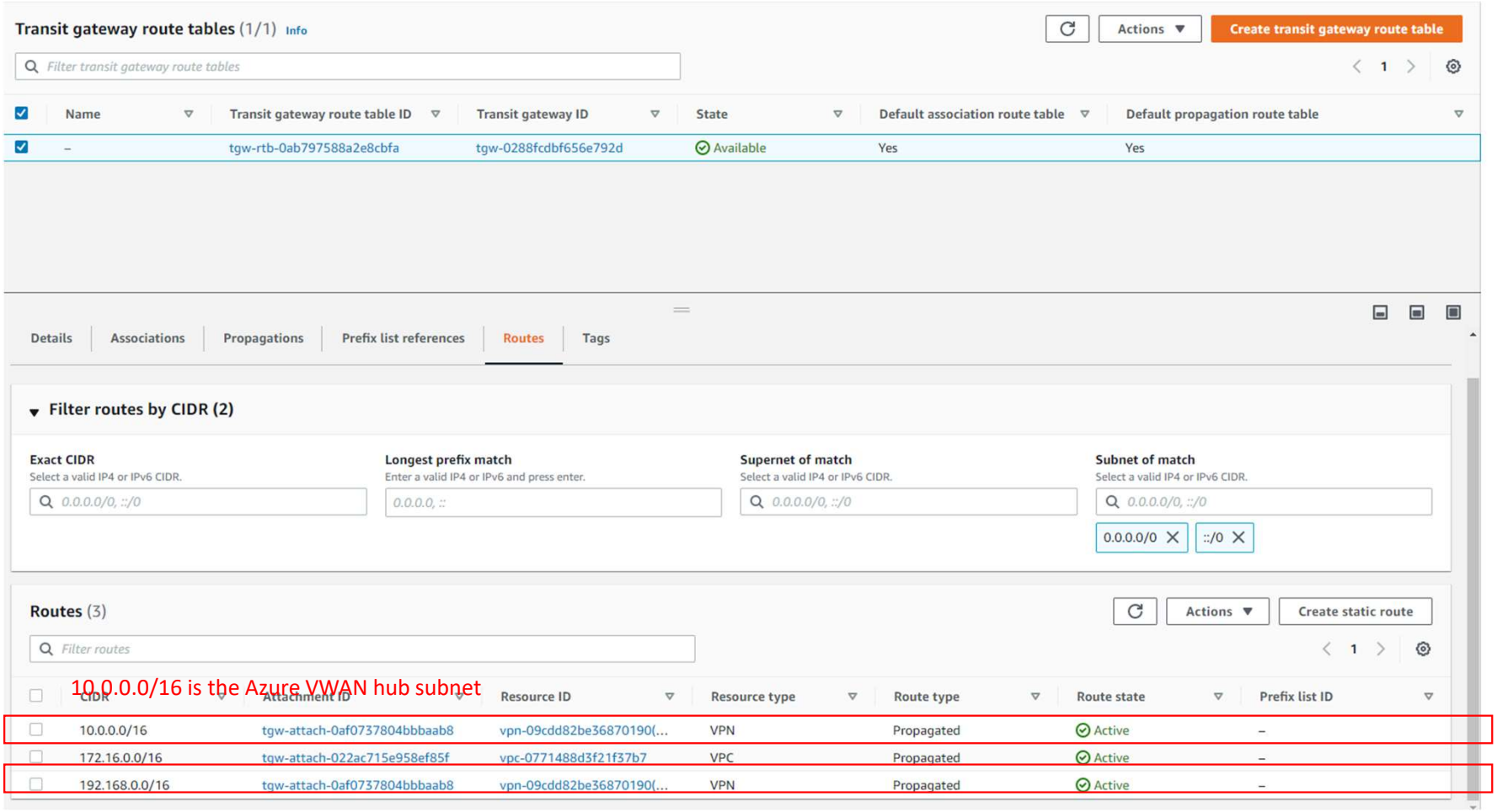


172.16.0.0/16 is the AWS VPC prefix

192.168.0.0/16 is from a connected spoke in the VWAN, this will auto-propagate to AWS

AWS route table on TGW

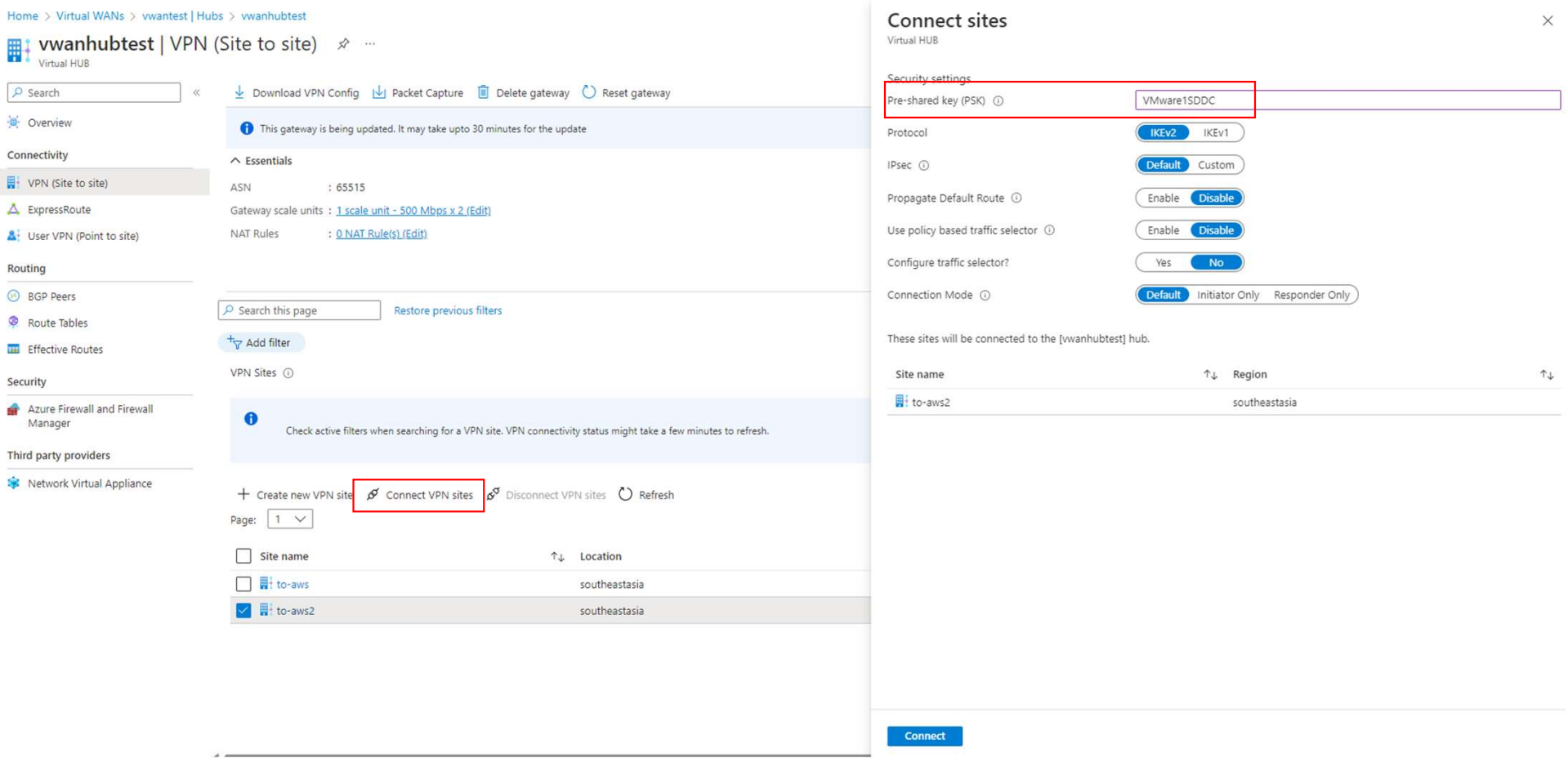
Both 10.0.0.0/16 and 192.168.0.0/16 are received from Azure



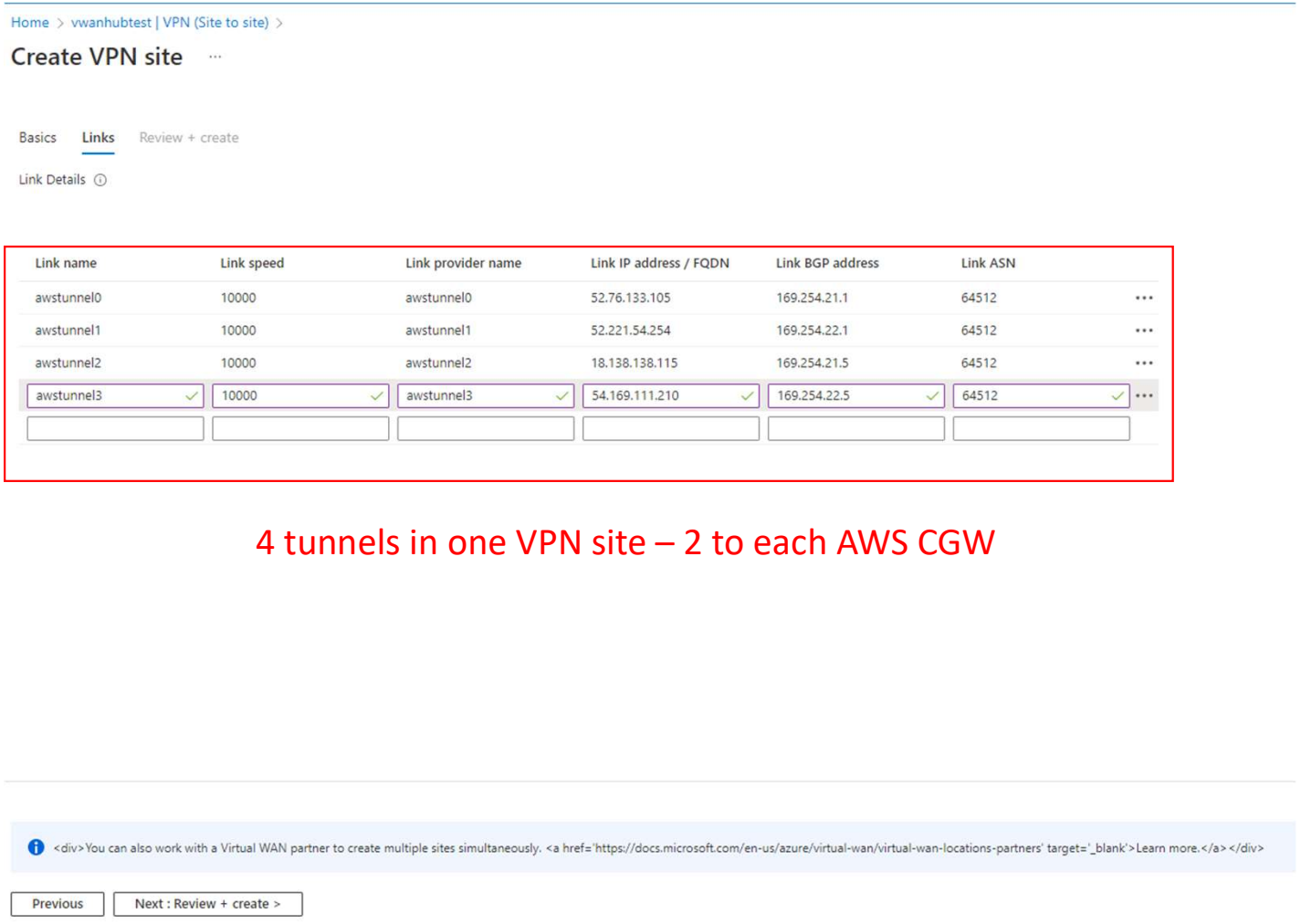
192.168.0.0/16 is the Azure spoke subnet that's connected to VWAN hub

Other points to note – how to key in PSK in Azure

In Azure, after you create the S2S VPN, you have to “connect VPN site” first before the option to enter PSK shows

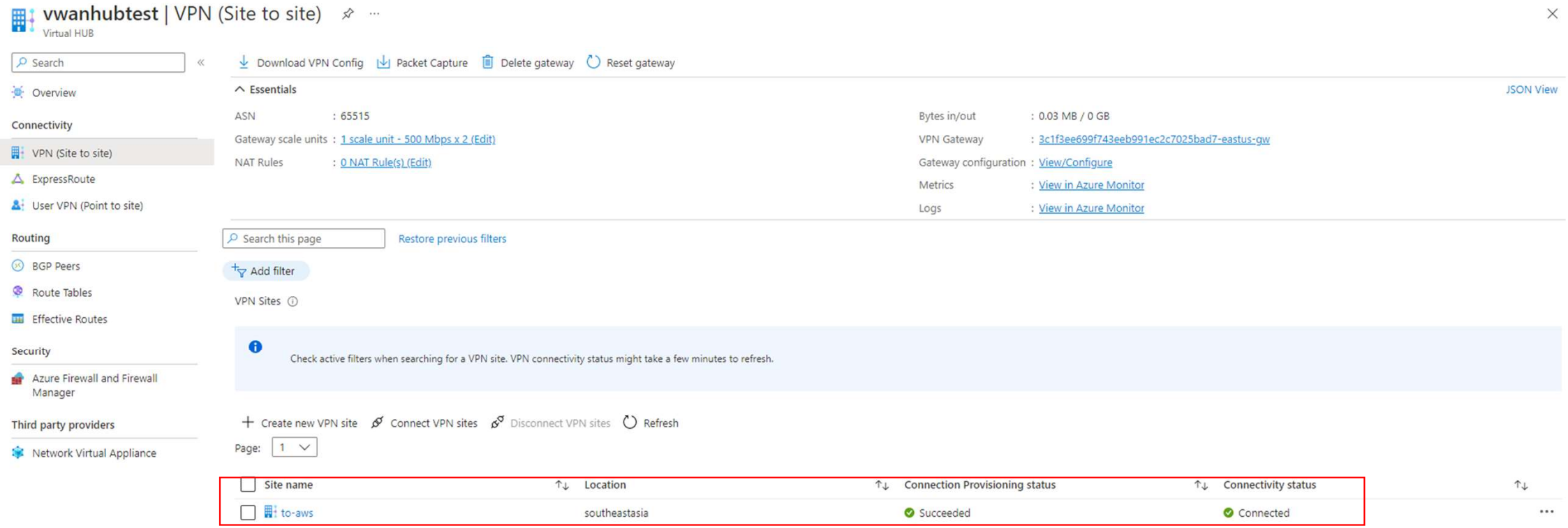


Other points to note – create a single VPN site in Azure with 4 tunnels – 2 to each AWS CGW

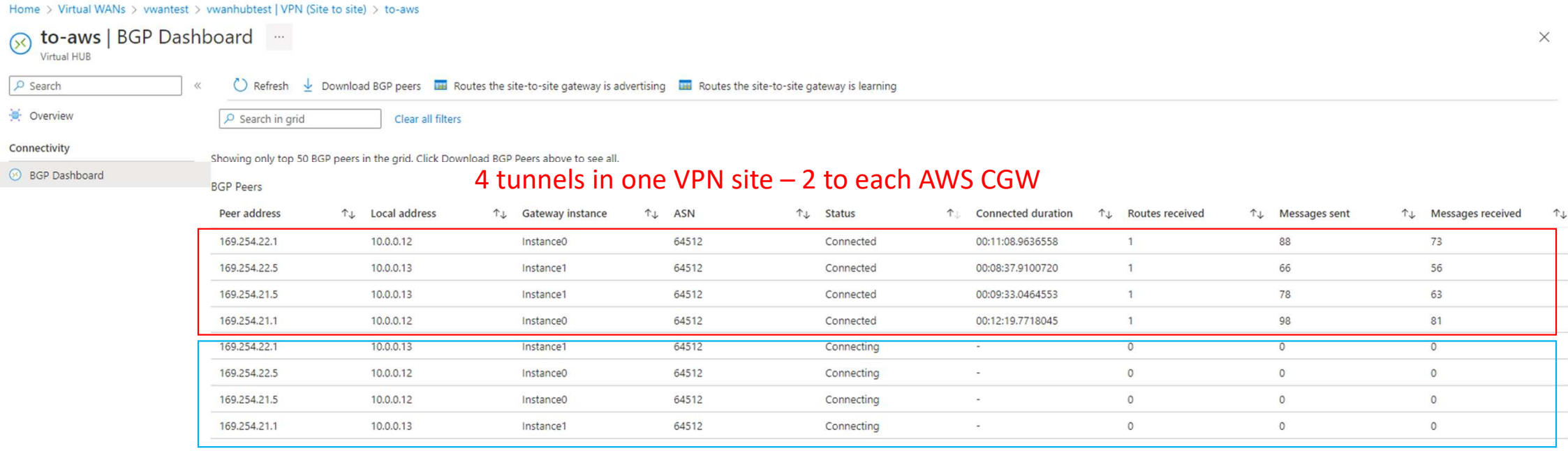


4 tunnels in one VPN site – 2 to each AWS CGW

Other points to note – create a single VPN site in Azure with 4 tunnels – 2 to each AWS CGW



Other points to note – create a single VPN site in Azure with 4 tunnels – 2 to each AWS CGW



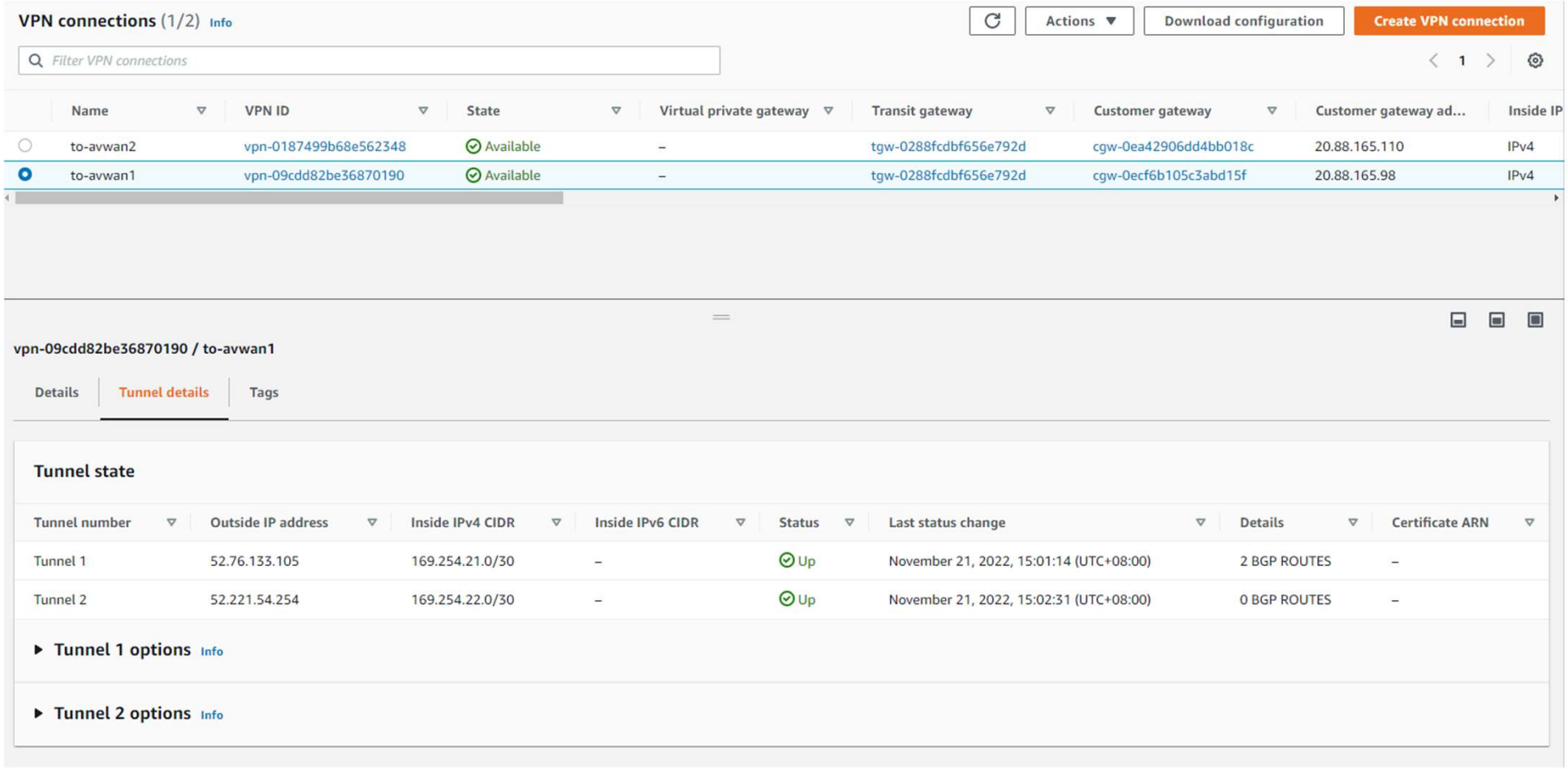
Peer address	Local address	Gateway instance	ASN	Status	Connected duration	Routes received	Messages sent	Messages received
169.254.22.1	10.0.0.12	Instance0	64512	Connected	00:11:08.9636558	1	88	73
169.254.22.5	10.0.0.13	Instance1	64512	Connected	00:08:37.9100720	1	66	56
169.254.21.5	10.0.0.13	Instance1	64512	Connected	00:09:33.0464553	1	78	63
169.254.21.1	10.0.0.12	Instance0	64512	Connected	00:12:19.7718045	1	98	81
169.254.22.1	10.0.0.13	Instance1	64512	Connecting	-	0	0	0
169.254.22.5	10.0.0.12	Instance0	64512	Connecting	-	0	0	0
169.254.21.5	10.0.0.12	Instance0	64512	Connecting	-	0	0	0
169.254.21.1	10.0.0.13	Instance1	64512	Connecting	-	0	0	0

Azure seems to expect the below BGP peering
VPN GW instance0 --2tunnels-- CGW1
VPN GW instance0 –2tunnels-- CGW2
VPN GW instance1 --2tunnels-- CGW1
VPN GW instance1–2tunnels-- CGW2

But AWS only expects the below
VPN GW instance0 --2tunnels-- CGW1
VPN GW instance1–2tunnels-- CGW2

Hence the discrepancy

Other points to note – create a single VPN site in Azure with 4 tunnels – 2 to each AWS CGW



Other points to note – create a single VPN site in Azure with 4 tunnels – 2 to each AWS CGW