AWS TRANSIT VPC

Version 1.1

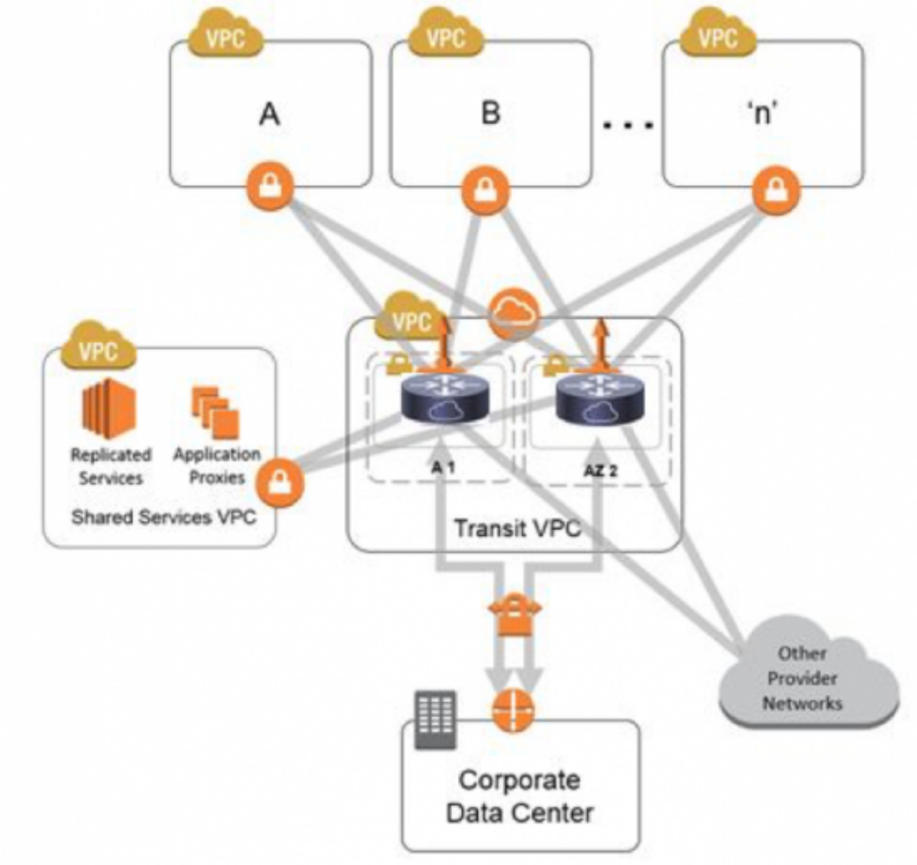
Table of Contents

INTRODUCTION

This documents demonstrates how to deploy a Cisco CSR transit VPC, and how to link it to multiple accounts along with topologies.

SCOPE

Transit VPC allows interconnectivity of multiple AWS VPC's from multiple Accounts, along with connectivity to an On Prem Data Center or a Multiple cloud environment (Azure). This teamed with a Shared Service VPC allows ease of management. A Shared Service VPC can host a Microsoft Domain Controller, Solarwinds Poller, Chef, Octopus, Matillion, System Center etc.. which will be able to communicate with all spoke VPC's along with Azure and On Prem.

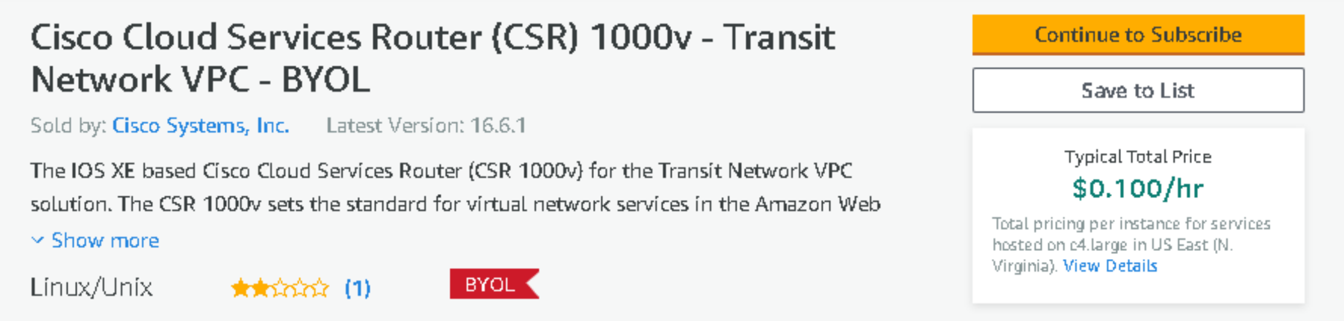


OVERVIEW

A transit VPC will allow dynamic routing between all spoke VPC's, on Prem, and multi cloud environment. When a new VPC is created it will automagically be added to our Transit VPC configuration, and have connectivity to Azure, On Prem, Shared Services and other Spoke VPC's.

INITAL CSR CONFIGURATION

Browse AWS Market Place for Cisco Cloud Services Router (CSR) 100v – Transit Network VPC, and Subscribe.



Cisco Cloud Services Router (CSR) 1000v - Transit Network VPC - BYOL

Sold by: Cisco Systems, Inc. Latest Version: 16.6.1

The IOS XE based Cisco Cloud Services Router (CSR 1000v) for the Transit Network VPC solution. The CSR 1000v sets the standard for virtual network services in the Amazon Web

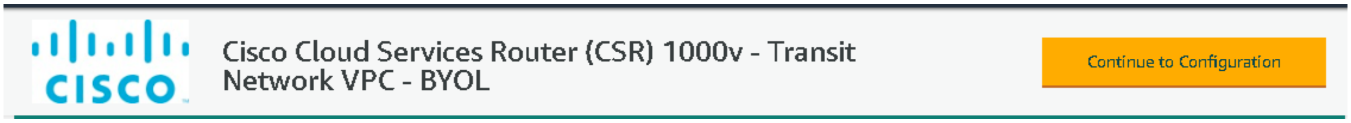
Typical Total Price

$0.100/hr

Total pricing per instance for services hosted on c4.large in US East (N. Virginia). View Details

Once Subscribed, accept Terms and Conditions.

It may take a few minutes for subscription to be linked to your account, once it is you will get a Continue to Configuration Option.



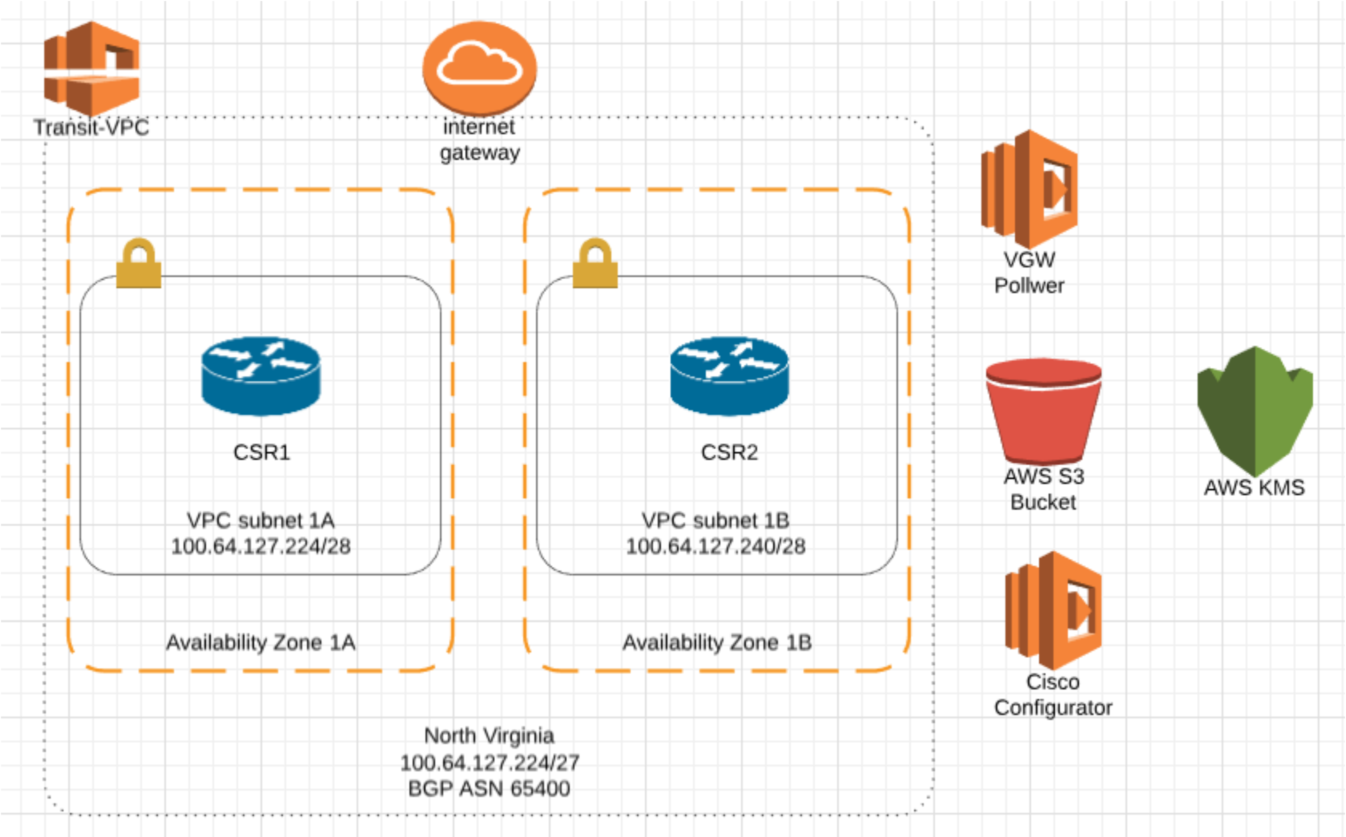
Cisco Cloud Services Router (CSR) 1000v - Transit Network VPC - BYOL

Fulfillment Options select Cloud Formation and Transit Network VPC with the CSR 1000V and Continue to Launch, then Launch Cloud Formation.

Name your Template Stack, ENV= Environment. (ENV-Transit-VPC)

For the Transit VPC Security Groups add the Philadelphia and Milford Public CIDR range to allow SSH access to CSR's. Default login is ec2-user with SSH Key pair.

TRANSIT VPC DESIGN



The transit VPC Cloud Formation template will use Carrier Grade NAT IP Range 100.64.0.0/10. The two CSR's are configured in an Active Standby configuration, where only one CSR will be routing at any given time. Three LAMBDA functions are also created.

Solution Helper which is invoked during Transit VPC Cloud Formation creation

VGW Poller looks at all your VGW's and search for a tag the one we will be using is 'transitvpc:spoke' when this tag is found it invoked Cisco Configurator.

Cisco Configurator creates the necessary ISAKMP, IPSEC, BGP, Security Group configuration on the CSR's when a tag is found.

REMOVING NON VALID CIPHERS

AWS supports several legacy ciphers we would not want to fall back to.

https://aws.amazon.com/blogs/aws/ec2-vpc-vpn-update-nat-traversal-additional-encryption-options-and-more/

Once the CSR's are spun up and accessible we will want to overwrite the isakmp and ipsec config to only use our required ciphers.

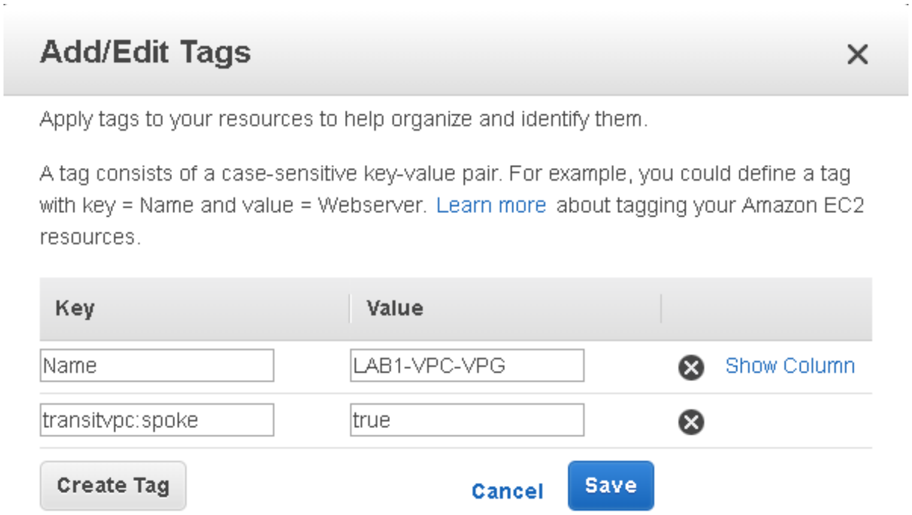
```
crypto ipsec transform-set ipsec-prop-vpn-aws esp-aes 256 esp-sha256-hmac
        mode tunnel
crypto ipsec profile ipsec-vpn-aws
set transform-set ipsec-prop-vpn-aws
        set pfs group2
crypto isakmp policy 200
        encr aes 256
        authentication pre-share
        group 2
        lifetime 28800
```

CONFIURING SPOKE VPC

Create your Virtual Private Gateway for your Spoke VPC, we should use our pre-defined ASN for the environment the VPC belongs to, Hub VPC should 65555.

Add / Edit Tags

Add in "transitvpc:spoke true'



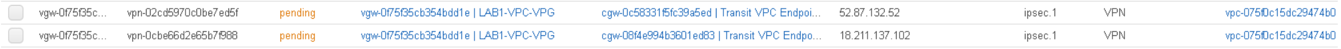
Add/Edit Tags

Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Amazon EC2 resources.

Key	Value	
Name	LAB1-VPC-VPG	⊗ Show Column
transitvpc:spoke	true	⊗

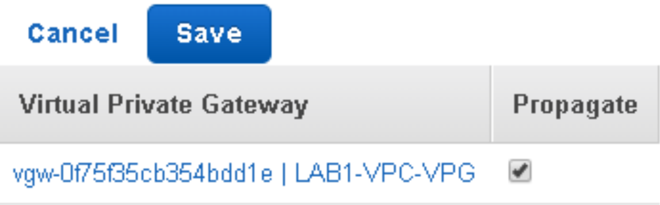
Once the Cisco Configurator locates your tag it will start provisioning the Site 2 Site VPN connections.



□	vgw-0f75f35c...	vpn-02cd5970c0be7ed5f	pending	vgw-0f75f35cb354bdd1e | LAB1-VPC-VPG	cgw-0c58331f5fc39a5ed | Transit VPC Endpoi...	52.87.132.52	ipsec.1	VPN	vpc-075f0c15dc29474b0
□	vgw-0f75f35c...	vpn-0cbe66d2e65b7f988	pending	vgw-0f75f35cb354bdd1e | LAB1-VPC-VPG	cgw-08f4e994b3601ed83 | Transit VPC Endpo...	18.211.137.102	ipsec.1	VPN	vpc-075f0c15dc29474b0

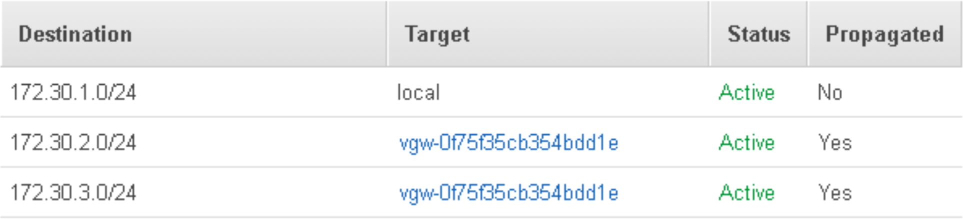
Under VPC Dashboard > Route Tables

Select the Route Table for your new VPC, to enable Dynamic Routing select Route Propagation.



Virtual Private Gateway	Propagate
vgw-0f75f35cb354bdd1e | LAB1-VPC-VPG	☑

This will allow the CSR's learned routes to be advertised into the VPC, if this not checked; the VPC's CIDR range will be advertised into the VPC, except the VPC will not learn propagated routes. It may take up to 10 minutes to see routes in the routing table due to VPN Connections taking a while to create.



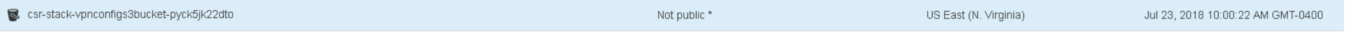
Destination	Target	Status	Propagated
172.30.1.0/24	local	Active	No
172.30.2.0/24	vgw-0f75f35cb354bdd1e	Active	Yes
172.30.3.0/24	vgw-0f75f35cb354bdd1e	Active	Yes

SCRIPT TO DEPLOY VGW ANSIBLE

https://github.com/SyrusHCW/ansible/blob/master/ansible-aws/VPN/VPC-VGW.yml

CONNECTING ANOTHER SUBSCRIPTION TO TRANSIT VPC

Browse Amazon S3 Buckets and select your CSR-STACK-VPNCONFIG



csr-stack-vpnconfigs3bucket-pyck5jk22dto	Not public *	US East (N. Virginia)	Jul 23, 2018 10:00:22 AM GMT-0400

Select Permissions for Bucket Policy

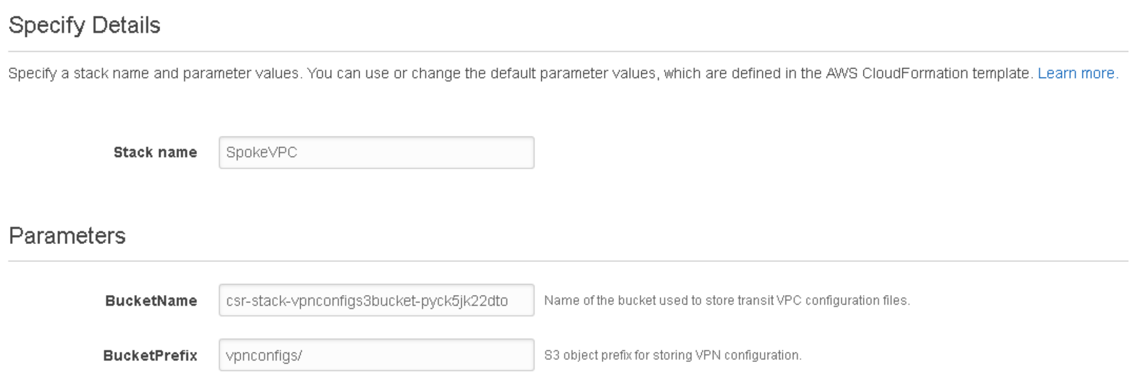
Add additional accounts under Principal (in this screen shot xxxxxxxxxxx is the second account)

Next go to IAM and select Encryption keys, select CSR-STACK-Key. Add the Second Account Principal.

Once this is completed, you can use

https://console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/new?&templateURL=https://s3.amazonaws.com/solutions-reference/transit-vpc/latest/transit-vpc-second-account.template

to deploy the VGW poller to the Second account using an S3 bucket.



Specify Details

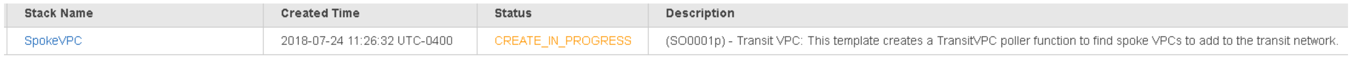
Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name	SpokeVPC	

Parameters

BucketName	csr-stack-vpnconfigs3bucket-pyck5jk22dto	Name of the bucket used to store transit VPC configuration files.
BucketPrefix	vpnconfigs/	S3 object prefix for storing VPN configuration.

The Bucket name needs to match the S3 Bucket from the Account running the Transit VPC. The Spoke VPC Stack will then be created.



Stack Name	Created Time	Status	Description
SpokeVPC	2018-07-24 11:26:32 UTC-0400	CREATE_IN_PROGRESS	(SO0001p) - Transit VPC: This template creates a TransitVPC poller function to find spoke VPCs to add to the transit network.

From this point forward you would create a VGW with Tags to create the VPN.

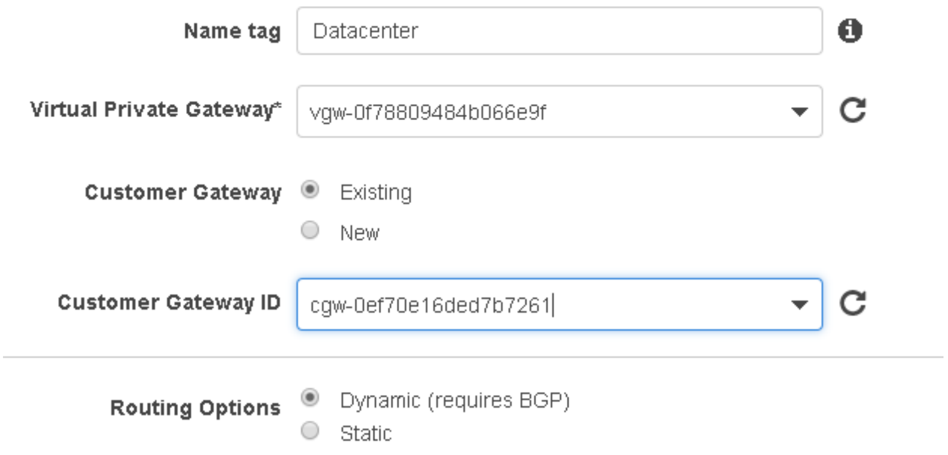
CONNECTING TRANSIT VPC TO DATACENTER

Connecting the Transit VPC to an On Prem Data Center Operates a little differently. A Virtual Private Gateway will need to be created that is detached from any VPC, the ASN will need to match the ASN of the Transit VPC.

Once Created add the VGW tags for “transitvpc:spoke true” Once the tag is read this detached VGW will create a VPN to the CSR along with learn and advertise routes.

To create the actual VPN connection create a Customer Gateway to your Datacenter.

Once Customer Gateway and VPG are created establish a VPN connections using these two devices.



Name tag: Datacenter

Virtual Private Gateway*: vgw-0f78809484b066e9f

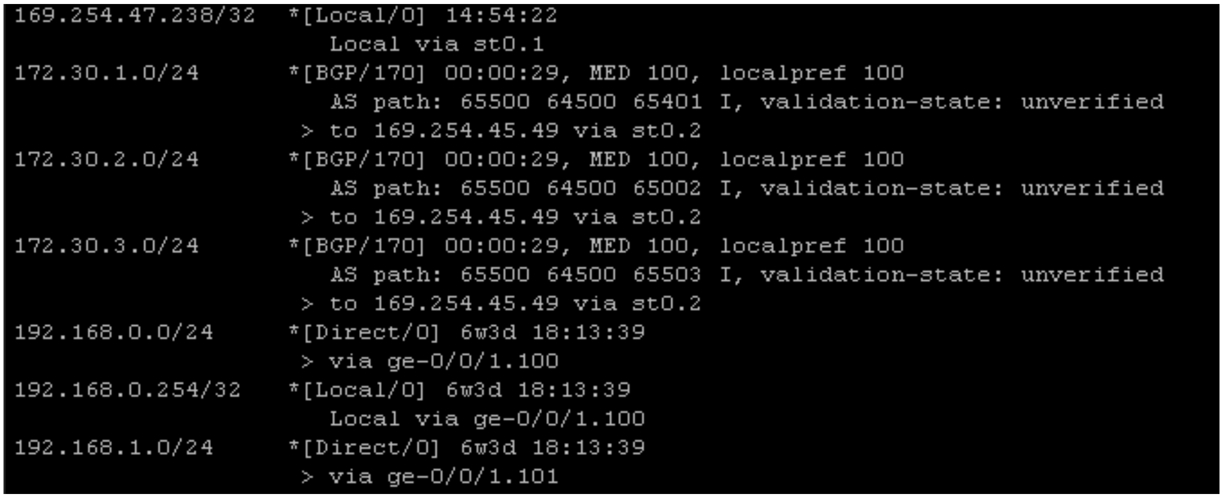
Customer Gateway: ● Existing ○ New

Customer Gateway ID: cgw-0ef70e16ded7b7261

Routing Options: ● Dynamic (requires BGP) ○ Static

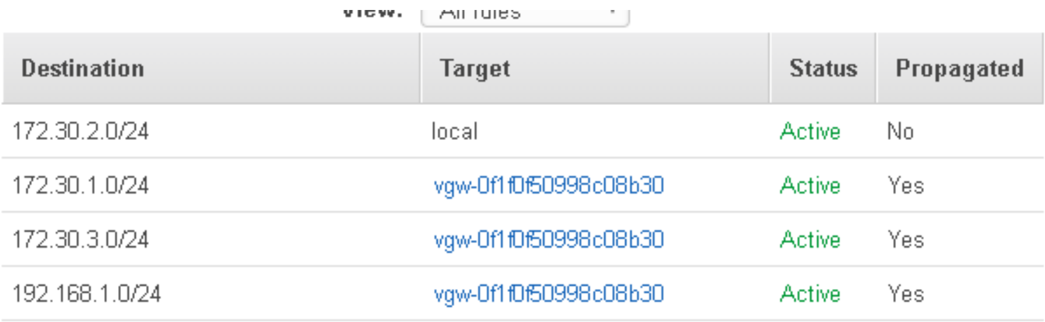
Once the VPN is established routes will be advertised to both sides.

Datacenter Side



```
169.254.47.238/32  *[Local/0] 14:54:22
                      Local via st0.1
172.30.1.0/24      *[BGP/170] 00:00:29, MED 100, localpref 100
                      AS path: 65500 64500 65401 I, validation-state: unverified
                    > to 169.254.45.49 via st0.2
172.30.2.0/24      *[BGP/170] 00:00:29, MED 100, localpref 100
                      AS path: 65500 64500 65002 I, validation-state: unverified
                    > to 169.254.45.49 via st0.2
172.30.3.0/24      *[BGP/170] 00:00:29, MED 100, localpref 100
                      AS path: 65500 64500 65503 I, validation-state: unverified
                    > to 169.254.45.49 via st0.2
192.168.0.0/24     *[Direct/0] 6w3d 18:13:39
                    > via ge-0/0/1.100
192.168.0.254/32   *[Local/0] 6w3d 18:13:39
                      Local via ge-0/0/1.100
192.168.1.0/24     *[Direct/0] 6w3d 18:13:39
                    > via ge-0/0/1.101
```

AWS Side



View: All rules

Destination	Target	Status	Propagated
172.30.2.0/24	local	Active	No
172.30.1.0/24	vgw-0f1f0f50998c08b30	Active	Yes
172.30.3.0/24	vgw-0f1f0f50998c08b30	Active	Yes
192.168.1.0/24	vgw-0f1f0f50998c08b30	Active	Yes

CONNECTING TRANSIT VPC TO AZURE

An IKEv2 and IPSEC configuration will need to be applied to the CSR's.

```
crypto ikev2 proposal ikev2-proposal-azure
 encryption aes-cbc-256
 integrity sha256
 group 2
!
crypto ikev2 policy ikev2-policy-azure
 proposal ikev2-proposal-azure
!

crypto ipsec transform-set ipsec-prop-vpn-azure esp-aes 256 esp-sha256-hmac
 mode tunnel
```

NAT-T will also need to be configured, in order to allow Azure to connect.

```
crypto ipsec nat-transparency udp-encapsulation

crypto ipsec df-bit clear
```

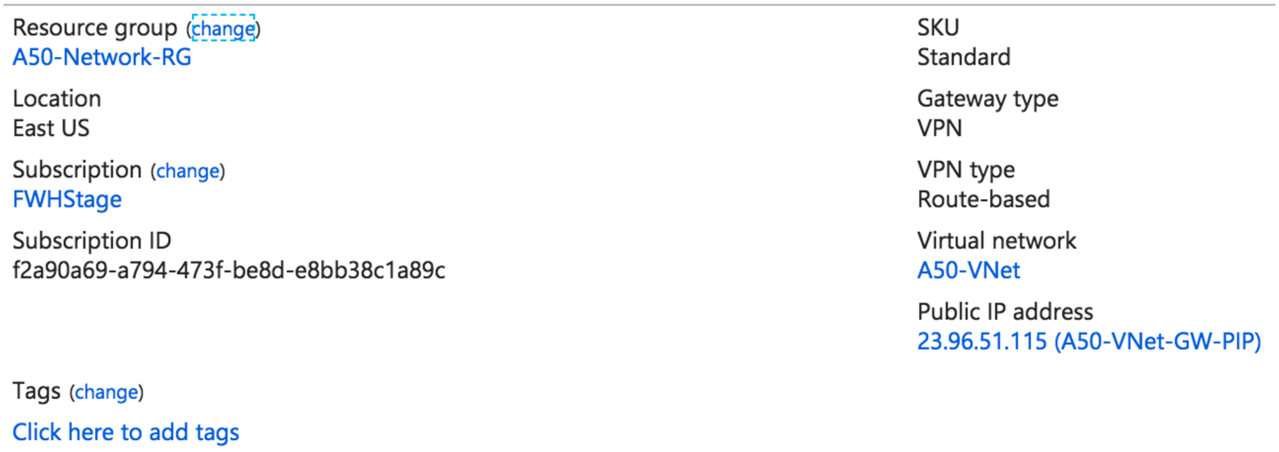
BUILDING CONFIGURATION SCRIPT VARIABLES

Script location: https://github.com/SyrusHCW/ansible/tree/master/transit-vpc

vnet: A50
This will be the name of your Azure VNet

tunnel_id : '100'
This is the numeric value for your Tunnel interface, this will create a new interface Tunnel100

azure_gw_ip: '23.96.51.115'
This will be the PIP address of your Azure Gateway



Resource group (change)
A50-Network-RG

Location
East US

Subscription (change)
FWHStage

Subscription ID
f2a90a69-a794-473f-be8d-e8bb38c1a89c

Tags (change)
Click here to add tags

SKU
Standard

Gateway type
VPN

VPN type
Route-based

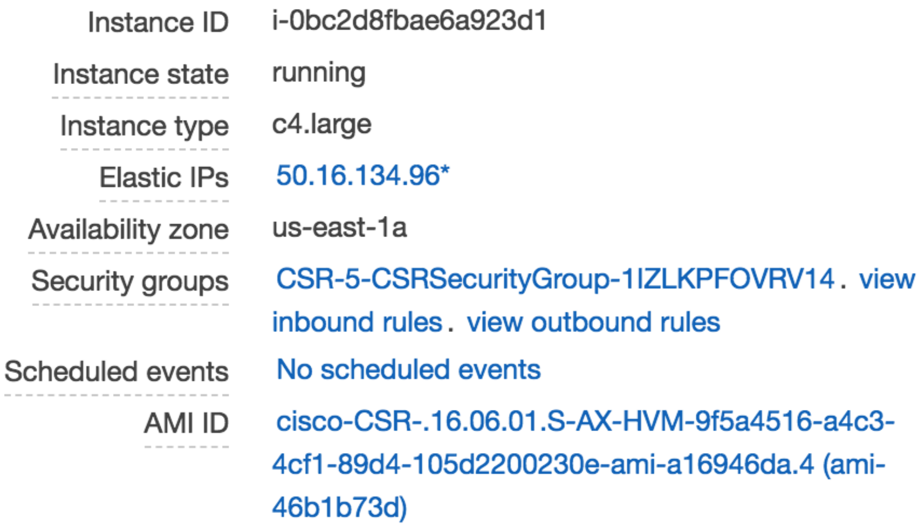
Virtual network
A50-VNet

Public IP address
23.96.51.115 (A50-VNet-GW-PIP)

vpn_psk: 'MASKED'

Specify your VPN preshared key

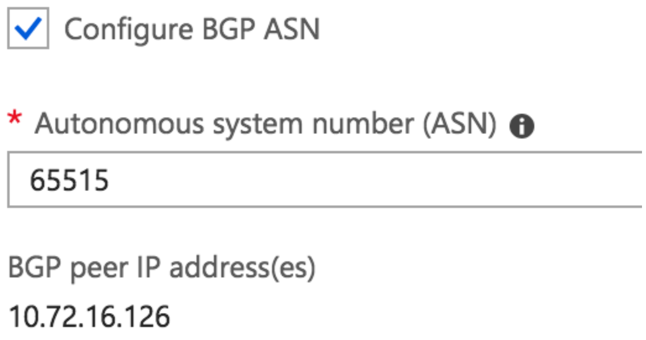
aws_csr_ip: '50.16.134.96'
This is your EIP for the AWS CSR



Instance ID	i-0bc2d8fbae6a923d1
Instance state	running
Instance type	c4.large
Elastic IPs	50.16.134.96*
Availability zone	us-east-1a
Security groups	CSR-5-CSRSecurityGroup-1IZLKPFOVRV14 . view inbound rules . view outbound rules
Scheduled events	No scheduled events
AMI ID	cisco-CSR-.16.06.01.S-AX-HVM-9f5a4516-a4c3-4cf1-89d4-105d2200230e-ami-a16946da.4 (ami-46b1b73d)

tunnel_ip: '172.30.255.254'
This will be the IP address of interface Tunnel100, this will be a host address, and the BGP Peering address for Azure.
Caveat for this address.
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vpn-faq
What are the requirements for the BGP Peer IP addresses on my VPN device?
Your on-premises BGP peer address MUST NOT be the same as the public IP address of your VPN device. Use a different IP address on the VPN device for your BGP Peer IP. It can be an address assigned to the loopback interface on the device, but please note that it cannot be an APIPA (169.254.x.x) address. Specify this address in the corresponding Local Network Gateway representing the location

az_bgp_ip: '10.72.16.126'
What address does Azure VPN gateway use for BGP Peer IP?
The Azure VPN gateway will allocate a single IP address from the GatewaySubnet range defined for the virtual network. By default, it is the second last address of the range. For example, if your GatewaySubnet is 10.12.255.0/27, ranging from 10.12.255.0 to 10.12.255.31, the BGP Peer IP address on the Azure VPN gateway will be 10.12.255.30. You can find this information when you list the Azure VPN gateway information.
For this example, my Gateway Subnet CIDR is 10.72.16.0/25, my BGP neighbor will be 10.72.16.126. This can also be located in the Azure Portal under Virtual Network Gateway/ Configuration



☑ Configure BGP ASN

* Autonomous system number (ASN)

65515

BGP peer IP address(es)

10.72.16.126

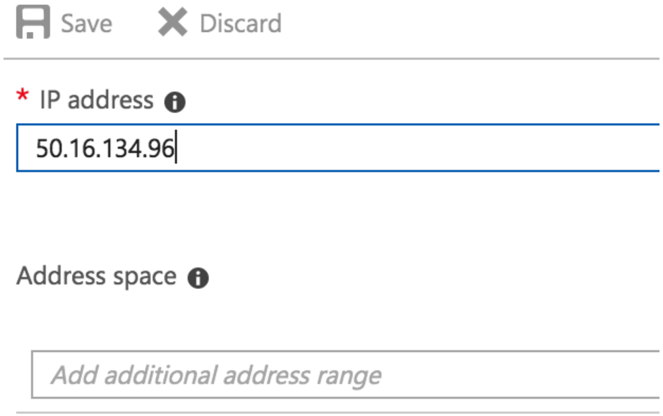
az_asn: '65515'
This should be configured using and ASN in the private range, Azure does several reserved ASN's we cannot use or peer with
Are there ASNs reserved by Azure?
Yes, the following ASNs are reserved by Azure for both internal and external peerings:
Public ASNs: 8074, 8075, 12076
Private ASNs: 65515, 65517, 65518, 65519, 65520

You cannot specify these ASNs for your on premises VPN devices when connecting to Azure VPN gateways.
Are there any other ASNs that I can't use?
Yes, the following ASNs are reserved by IANA and can't be configured on your Azure VPN Gateway:
23456, 64496-64511, 65535-65551

Built Configuration using variables

```
ip vrf vpn-azure-A50-vpn
 rd 65555:100
 route-target export 65555:0
 route-target import 65555:0
exit
crypto ikev2 keyring ikev2-key-azure-A50
 peer 23.96.51.115
  address 23.96.51.115
  pre-shared-key MASKED
exit
exit
crypto ikev2 profile ikev2-profile-azure-A50
 match identity remote address 23.96.51.115 255.255.255.255
 identity local address 50.16.134.96
 authentication remote pre-share
 authentication local pre-share
 keyring local ikev2-key-azure-A50
 lifetime 28800
 dpd 10 5 on-demand
exit
crypto ipsec profile ipsec-profile-azure-A50
 set security-association lifetime kilobytes 102400000
 set transform-set ipsec-prop-vpn-azure
 set ikev2-profile ikev2-profile-azure-A50
exit
interface Tunnel100
 description vpn from Azure A50 Vnet
 ip vrf forwarding vpn-azure-A50-vpn
 ip address 172.30.255.254 255.255.255.255
 ip tcp adjust-mss 1350
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 23.96.51.115
 tunnel protection ipsec profile ipsec-profile-azure-A50
 ip virtual-reassembly
exit
router bgp 65555
 bgp log-neighbor-changes
 !
 address-family ipv4 vrf vpn-azure-A50-vpn
  neighbor 10.72.16.126 remote-as 65515
  neighbor 10.72.16.126  ebgp-multihop 255
  neighbor 10.72.16.126  update-source Tunnel100
  neighbor 10.72.16.126  activate
 exit-address-family
!
 exit
ip route vrf vpn-azure-A50-vpn 10.72.16.126  255.255.255.255 Tunnel100
```

**If you have multiple gateways associated with your Gateway Subnet and it has address space specified, this will be advertised into BGP.



* IP address
50.16.134.96

Address space

Add additional address range

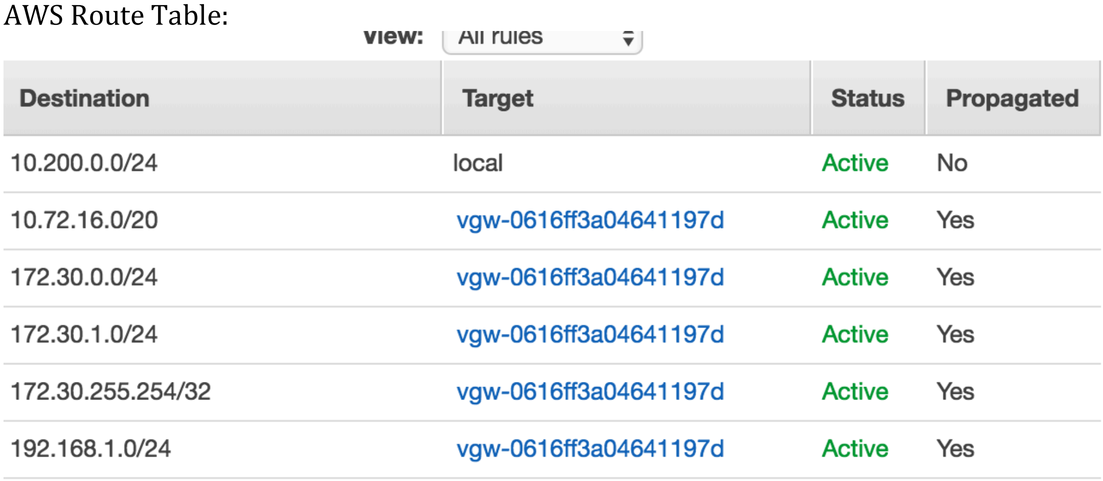
CONFIRMING BGP

Routes:

192.168.1.0/24 is Connected to a Juniper SRX (Data Center)
172.30.0.0/24 AWS VPC 1
172.30.1.0/24 AWS VPC 2

10.200.0.0/24 AWS VPC 3
10.72.10.0/20 Azure VNet A50

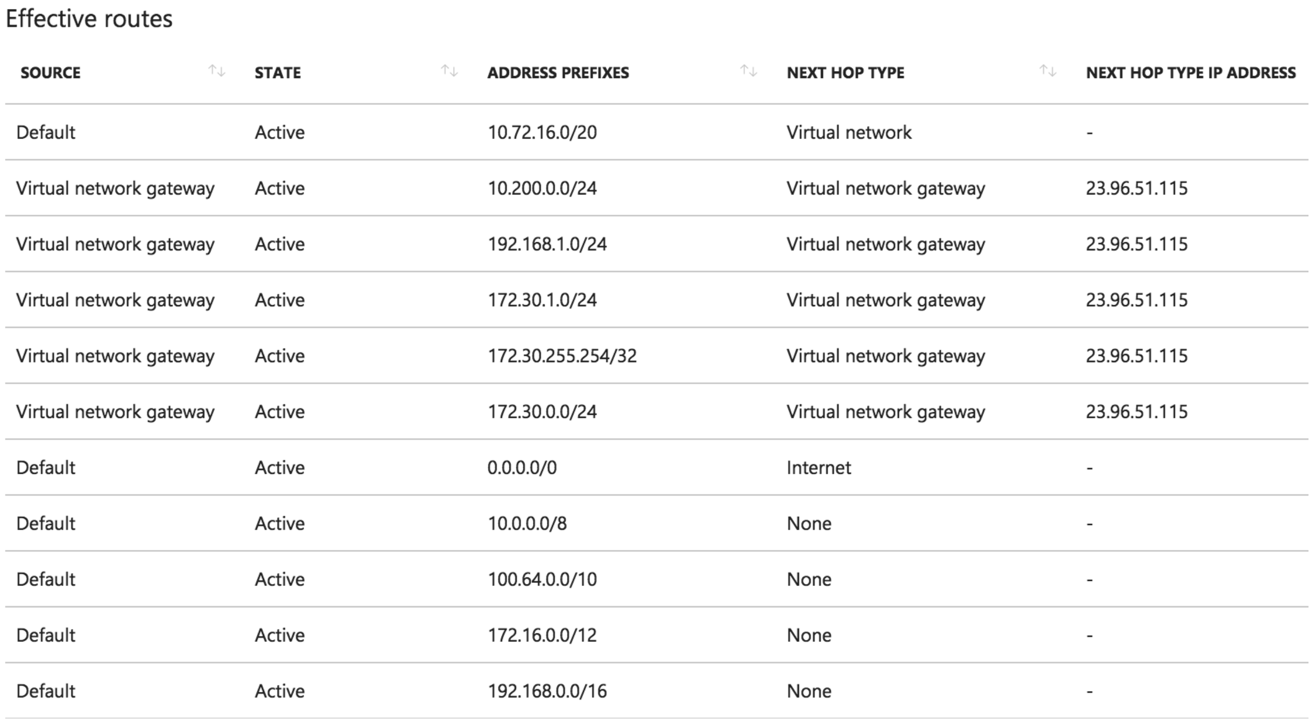
AWS Route Table:



View: All rules

Destination	Target	Status	Propagated
10.200.0.0/24	local	Active	No
10.72.16.0/20	vgw-0616ff3a04641197d	Active	Yes
172.30.0.0/24	vgw-0616ff3a04641197d	Active	Yes
172.30.1.0/24	vgw-0616ff3a04641197d	Active	Yes
172.30.255.254/32	vgw-0616ff3a04641197d	Active	Yes
192.168.1.0/24	vgw-0616ff3a04641197d	Active	Yes

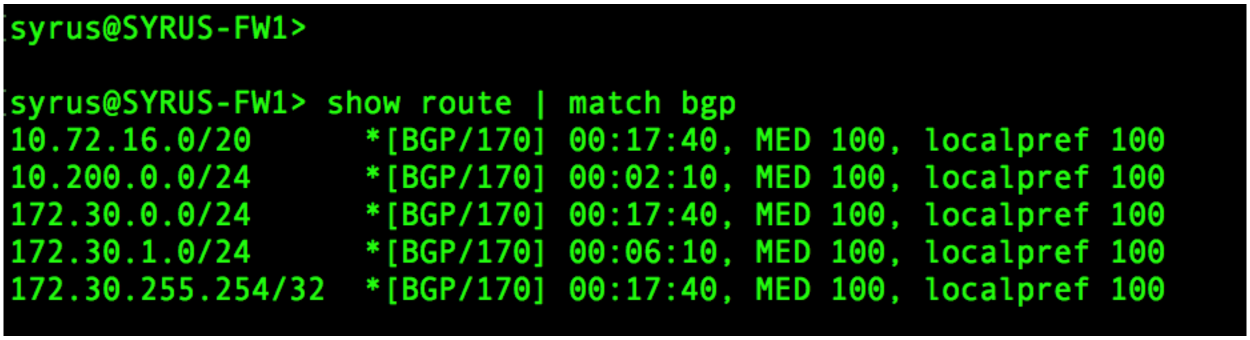
Azure: Although BGP routing will working in Azure without a Route table, if you want to see the routes that Azure learned you will need to create a Route Table and associate it to your Gateway Subnet.



Effective routes

SOURCE	STATE	ADDRESS PREFIXES	NEXT HOP TYPE	NEXT HOP TYPE IP ADDRESS
Default	Active	10.72.16.0/20	Virtual network	-
Virtual network gateway	Active	10.200.0.0/24	Virtual network gateway	23.96.51.115
Virtual network gateway	Active	192.168.1.0/24	Virtual network gateway	23.96.51.115
Virtual network gateway	Active	172.30.1.0/24	Virtual network gateway	23.96.51.115
Virtual network gateway	Active	172.30.255.254/32	Virtual network gateway	23.96.51.115
Virtual network gateway	Active	172.30.0.0/24	Virtual network gateway	23.96.51.115
Default	Active	0.0.0.0/0	Internet	-
Default	Active	10.0.0.0/8	None	-
Default	Active	100.64.0.0/10	None	-
Default	Active	172.16.0.0/12	None	-
Default	Active	192.168.0.0/16	None	-

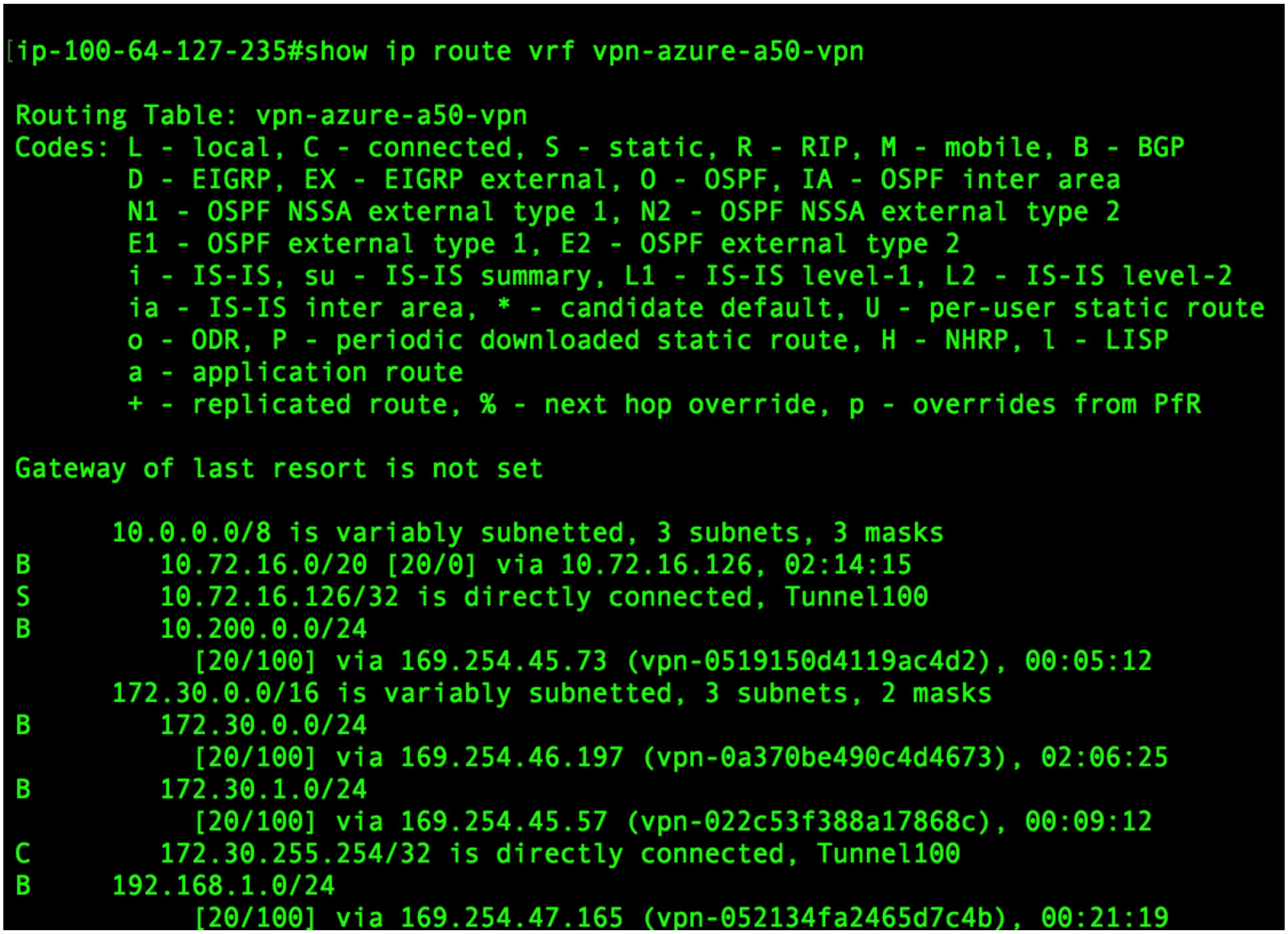
Juniper SRX:



```
[syrus@SYRUS-FW1>

[syrus@SYRUS-FW1> show route | match bgp
10.72.16.0/20      *[BGP/170] 00:17:40, MED 100, localpref 100
10.200.0.0/24      *[BGP/170] 00:02:10, MED 100, localpref 100
172.30.0.0/24      *[BGP/170] 00:17:40, MED 100, localpref 100
172.30.1.0/24      *[BGP/170] 00:06:10, MED 100, localpref 100
172.30.255.254/32  *[BGP/170] 00:17:40, MED 100, localpref 100
```

Cisco CSR:



```
[ip-100-64-127-235#show ip route vrf vpn-azure-a50-vpn

Routing Table: vpn-azure-a50-vpn
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
B        10.72.16.0/20 [20/0] via 10.72.16.126, 02:14:15
S        10.72.16.126/32 is directly connected, Tunnel100
B        10.200.0.0/24
           [20/100] via 169.254.45.73 (vpn-0519150d4119ac4d2), 00:05:12
      172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
B        172.30.0.0/24
           [20/100] via 169.254.46.197 (vpn-0a370be490c4d4673), 02:06:25
B        172.30.1.0/24
           [20/100] via 169.254.45.57 (vpn-022c53f388a17868c), 00:09:12
C        172.30.255.254/32 is directly connected, Tunnel100
B     192.168.1.0/24
           [20/100] via 169.254.47.165 (vpn-052134fa2465d7c4b), 00:21:19
```