



AT&T NetBond® for Amazon Web Services™

Service Activation Overview

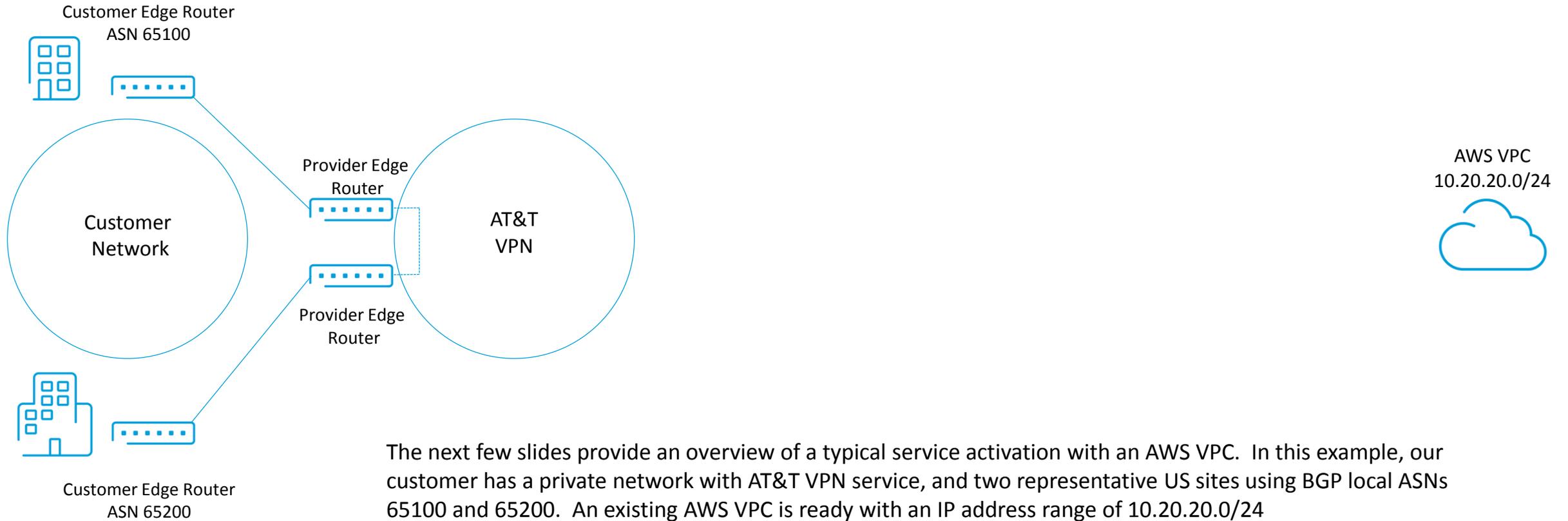
AT&T NetBond allows AT&T customers to extend their MPLS virtual private network to cloud services such as Amazon Web Services. With NetBond enabled, an AWS VPC™ or AWS™ public service such as S3™ will appear as another site on the VPN. Customers can then reach their EC2™ instances or S3 buckets with better scalability, improved security, and greater availability.

Using the AT&T Cloud Services Portal, the NetBond service can be quickly provisioned. The next few slides provide an overview to plan and enable the service.

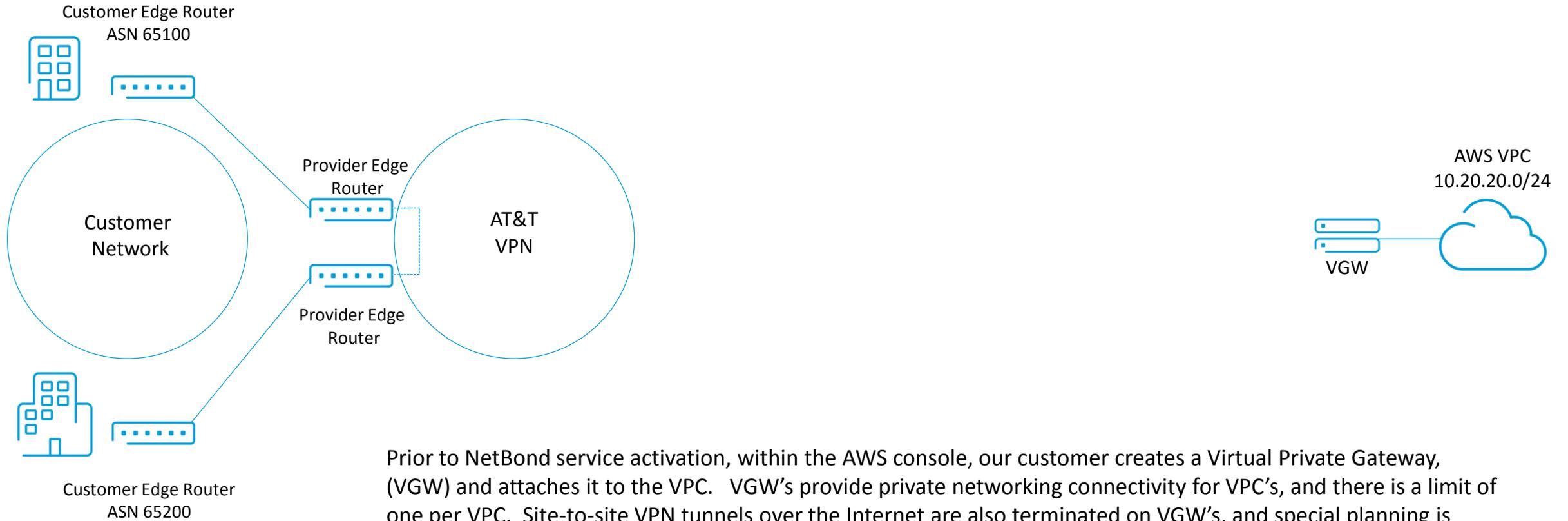
Prior to enablement, the customer should have or procure service with AWS. They should also work with the AT&T account team to sign up for NetBond cloud services. Upon contract signing, the customer will receive a welcome email for credentials to www.synaptic.att.com.

Service Activation Overview for AWS Virtual Private Cloud

Example Scenario – Customer with existing AT&T VPN and AWS VPC

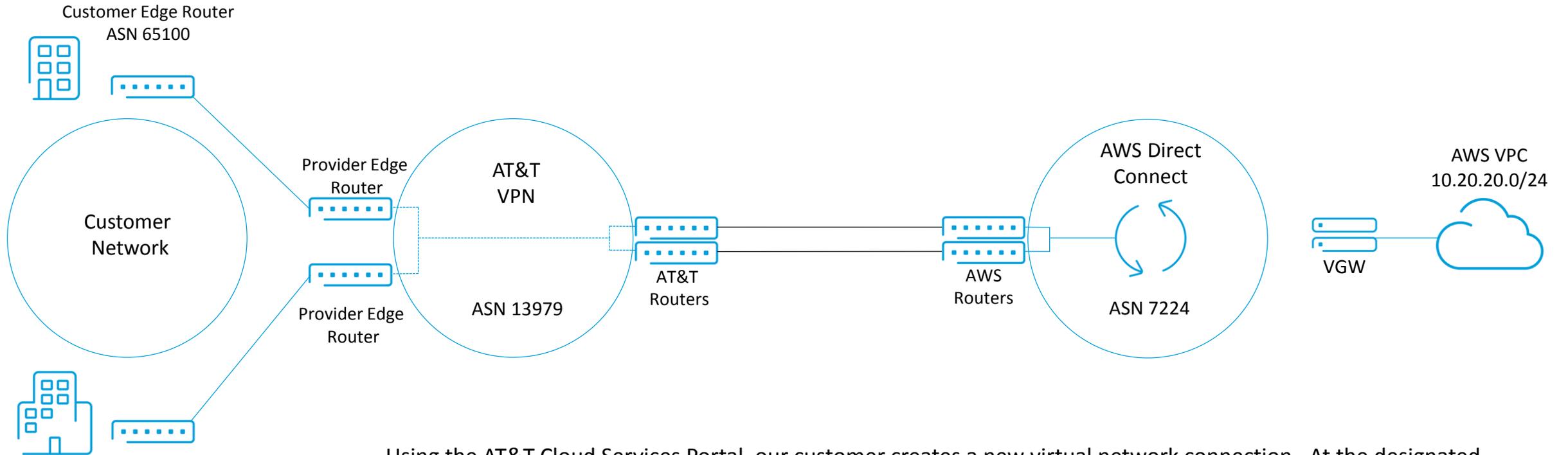


Prerequisite – Attach Virtual Private Gateway to VPC



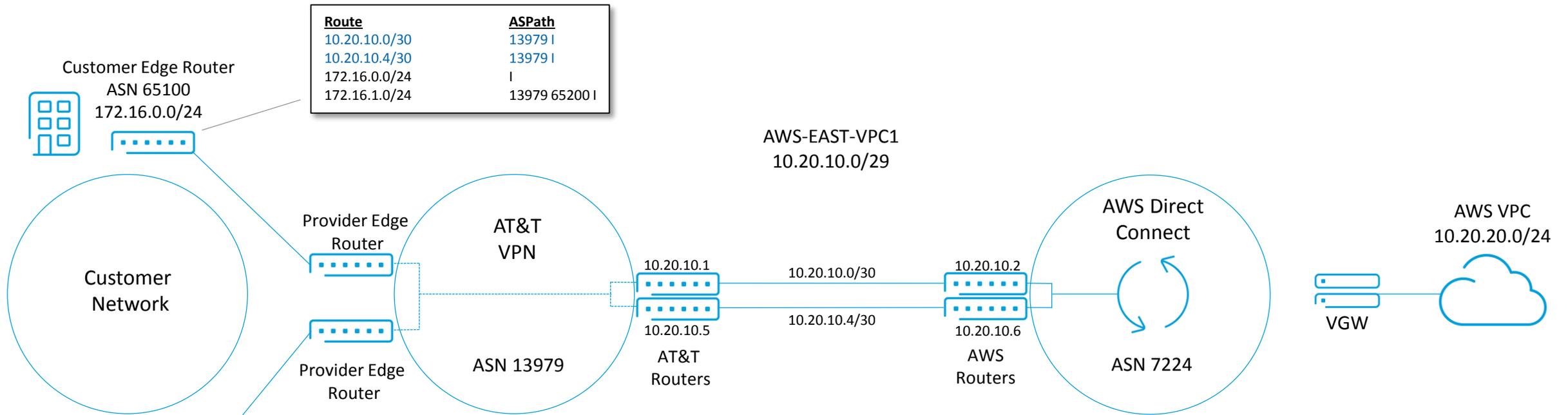
Prior to NetBond service activation, within the AWS console, our customer creates a Virtual Private Gateway, (VGW) and attaches it to the VPC. VGW's provide private networking connectivity for VPC's, and there is a limit of one per VPC. Site-to-site VPN tunnels over the Internet are also terminated on VGW's, and special planning is required if both IPSEC and NetBond will co-exist.

Step 1 – Create VNC



Using the AT&T Cloud Services Portal, our customer creates a new virtual network connection. At the designated region, NetBond orchestration enables our customer's private network on the AT&T routers at the meet-me point with the AWS routers. In addition, our customer chooses a minimum bandwidth commitment for the virtual network connection.

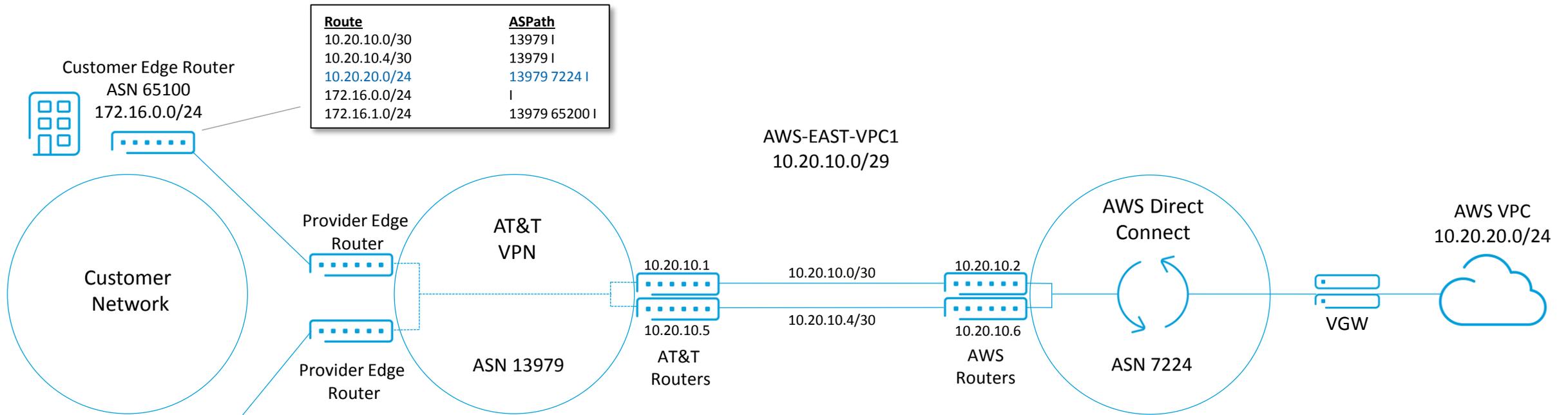
Step 2 – Create VLAN



Using the AWS account number and a /29 address block from their enterprise IP space, our customer creates a VLAN within the VNC. The /29 address block should not overlap any AWS VPC CIDR blocks. NetBond orchestration provisions a pair of connections between the virtual routing interface on the AT&T routers and the AWS Direct Connect service. The /29 space is automatically provisioned as two /30 subnets.

The customer edge routers will now see the /30 subnets in their routing tables. However the AWS VPC, (10.20.20.0/24 in the example), will not yet appear since the VPC is not connected to Direct Connect

Step 3 – Accepting Direct Connect Virtual Interfaces in AWS Console



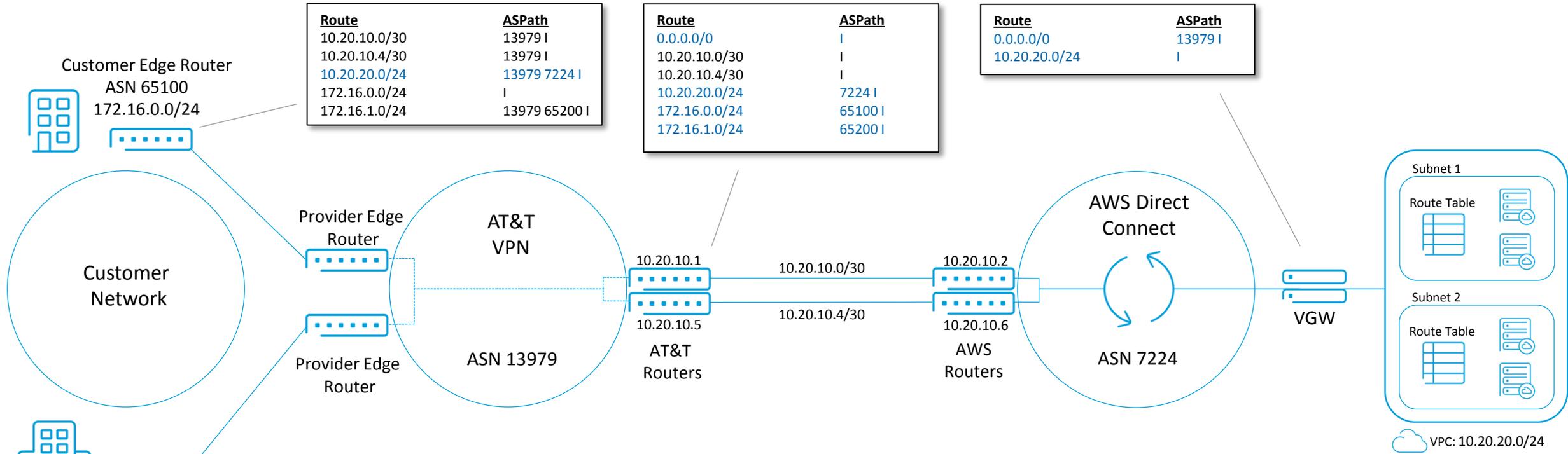
Route	ASPath
10.20.10.0/30	13979 I
10.20.10.4/30	13979 I
10.20.20.0/24	13979 7224 I
172.16.0.0/24	I
172.16.1.0/24	13979 65200 I

Within the AWS console, our customer’s AWS administrator will find two new Direct Connect Virtual Interfaces, (VIFs) with a status of “Pending Acceptance”. The virtual interface connection names will match the NetBond VLAN name, and the IP addresses will match the two /30’s. During acceptance, Amazon will prompt for the VGW to be linked to the virtual interfaces.

After a few minutes, AWS will finish provisioning the connections to the VGW, and the CIDR block associated with the VPC will be advertised to the MPLS VPN.

AWS Route Table Considerations

Step 4 – Update Amazon Route Tables for Each Subnet

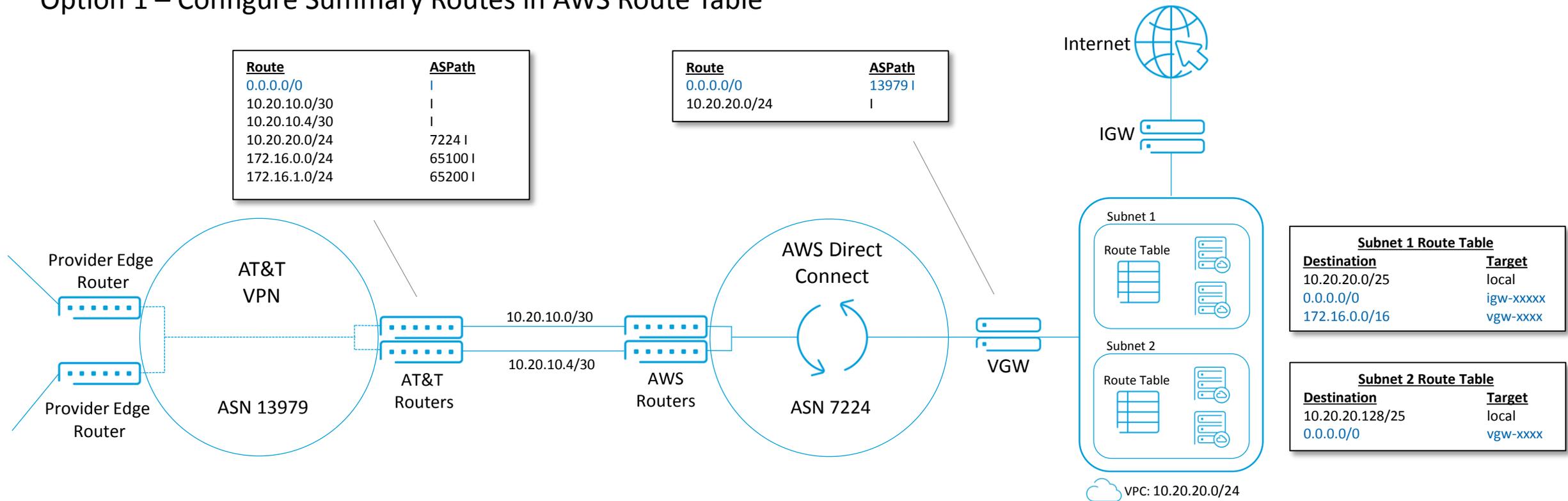


AWS Route Tables determine the routing configuration for EC2 instances in the associated subnet. They can be statically configured or can dynamically learn routes from the VGW route table.

The VGW route table cannot be directly configured, but only manipulated via route advertisements from Direct Connect connections or IPSEC VPN tunnels.

Since AWS limits routes to 100, special consideration must be given how to accept routes from AT&T to AWS. By default, AT&T NetBond routers retain all the customer routes, but only advertise the default route to AWS.

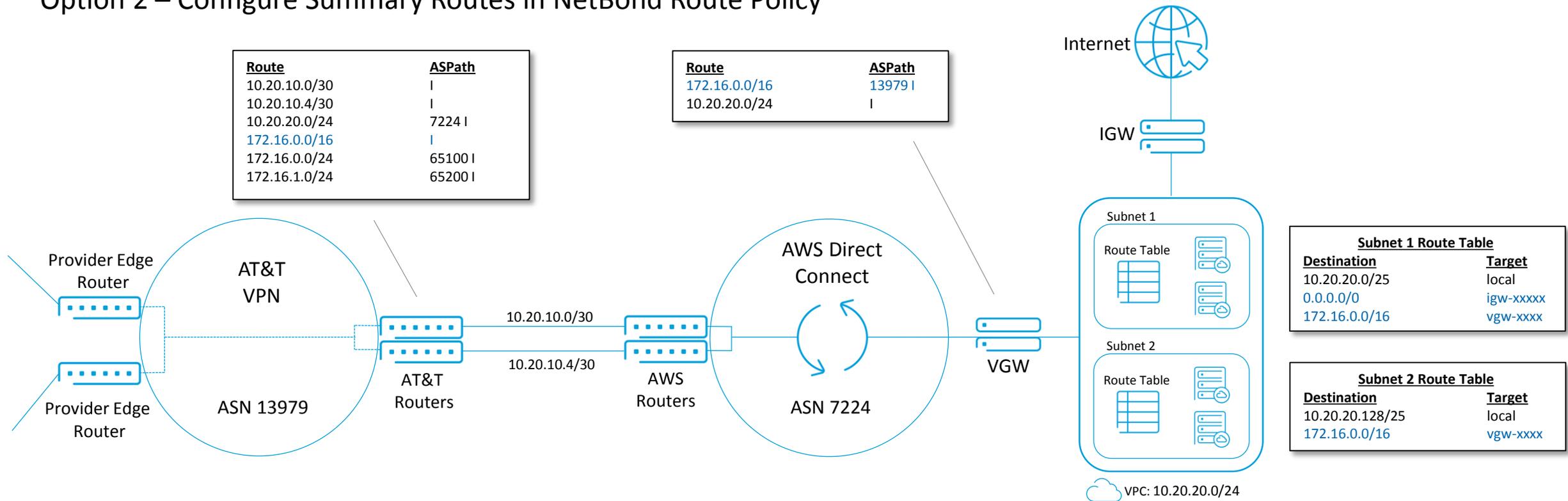
Option 1 – Configure Summary Routes in AWS Route Table



One option is for the AWS administrator to manage summary routes in the individual AWS route tables. Each route table should have route propagation disabled. The administrator can then configure routes and designate the target.

In our example, the customer has attached an AWS Internet Gateway, (IGW) to the VPC. They have configured the first subnet’s route table to use the IGW as the default gateway, and a summary route for their enterprise network with a target of the VGW. They have configured the second subnet’s route table to use the VGW as the default gateway for all traffic.

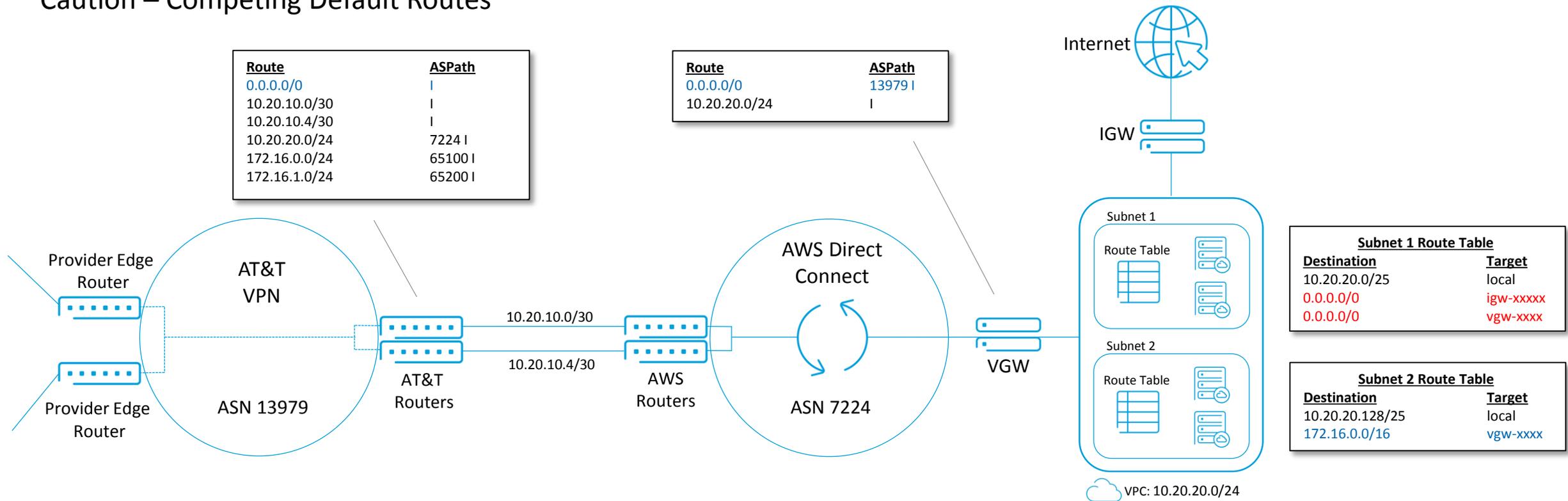
Option 2 – Configure Summary Routes in NetBond Route Policy



Another option is for the NetBond administrator to use NetBond’s route policy features to announce summary routes to the AWS VGW, and disable the default route announcement. (Note that there must be at least one route matching or more specific in the route table the AT&T routers to announce the route.) The VGW will only populate with the routes administered by the NetBond administrator.

Per route table, the AWS administrator can choose to dynamically learn the routes from the VGW or manually configure them. In our customer’s example, the AWS administrator chose to dynamically learn routes in both tables. They also chose not to add a default route to the IGW in the second routing table.

Caution – Competing Default Routes



By default, AT&T NetBond will announce the largest summary route possible – the default route. If the intent is for the subnet to use Amazon’s IGW to reach the Internet, and the NetBond administrator has left the default route to be advertised, it’s important for the AWS administrator to configure the route table to not learn routes dynamically from the VGW.

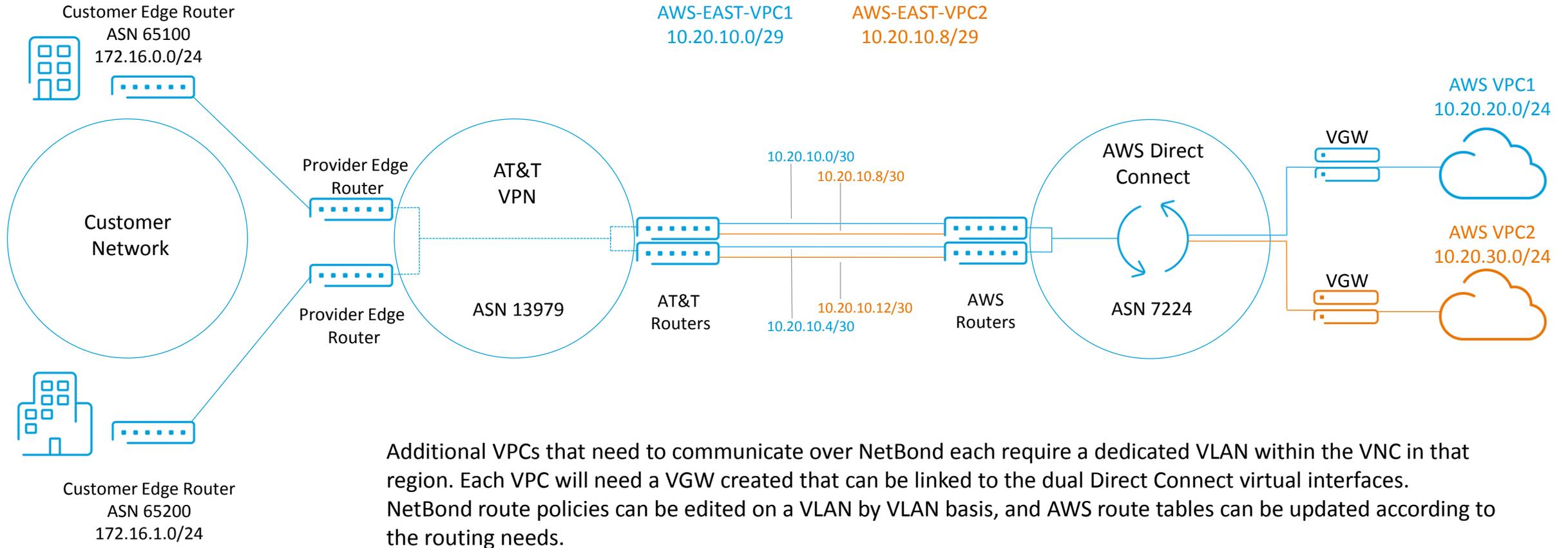
In the example above, the AWS administrator has mistakenly configured the first route table to learn routes dynamically from the VGW. Because the VGW has learned the default route from AT&T, the route table has two competing default routes.

Summary Steps

1. Obtain AWS service
2. Work with the AT&T account team to sign up for NetBond services. A welcome letter will provide credentials to AT&T Cloud Services Portal, (www.synaptic.att.com)
3. Within AWS, at least one VPC with an attached Virtual Private Gateway is required in a region collocated with NetBond.
4. Create NetBond Virtual Network Connection. (Required: Name of AT&T VPN, region, free-form name for Virtual Network Connection, and minimum bandwidth commitment)
5. Create NetBond VLAN. (Required: /29 address space, free-form name, and AWS account number)
6. Within AWS console's Direct Connect service, accept two new virtual interfaces to the Virtual Private Gateway.
(<http://docs.aws.amazon.com/directconnect/latest/UserGuide/accepthostedvirtualinterface.html>)
7. Determine summary routes that will be used to reach hosts on the AT&T MPLS VPN.
8. Configure the route tables to either a) allow route propagation from the Virtual Private Gateway, or b) manually configure summary routes with a target of the Virtual Private Gateway

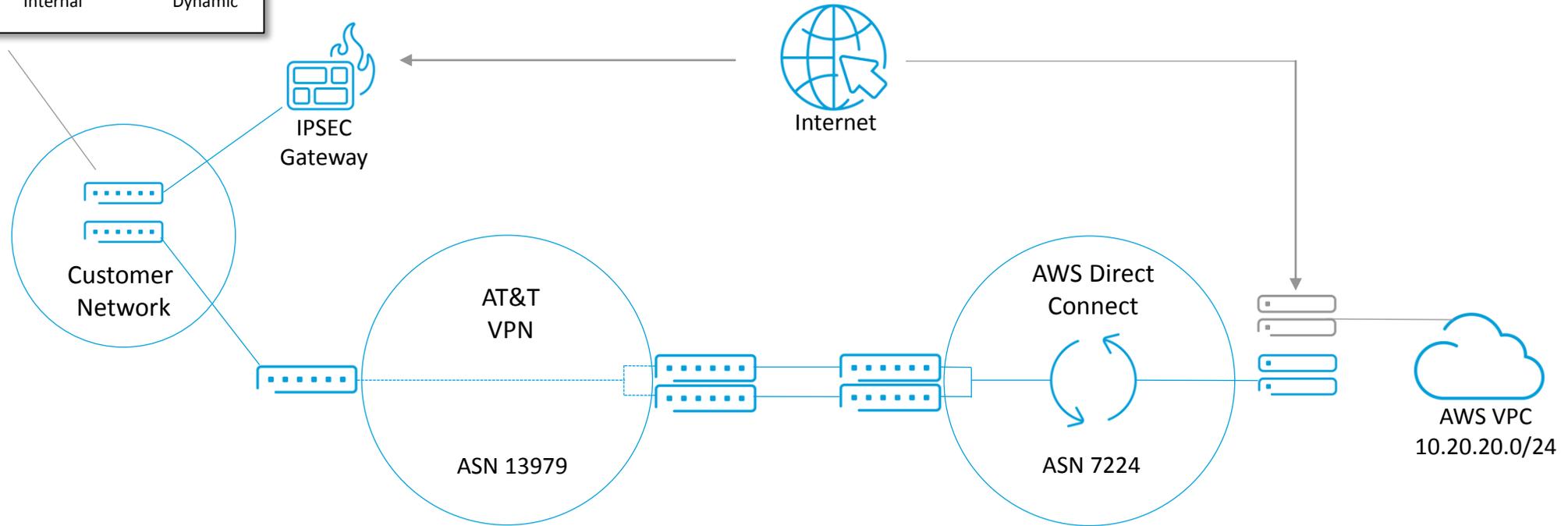
Technical Considerations

Additional VPCs



Migrating from Site to Site VPN Tunnels to NetBond

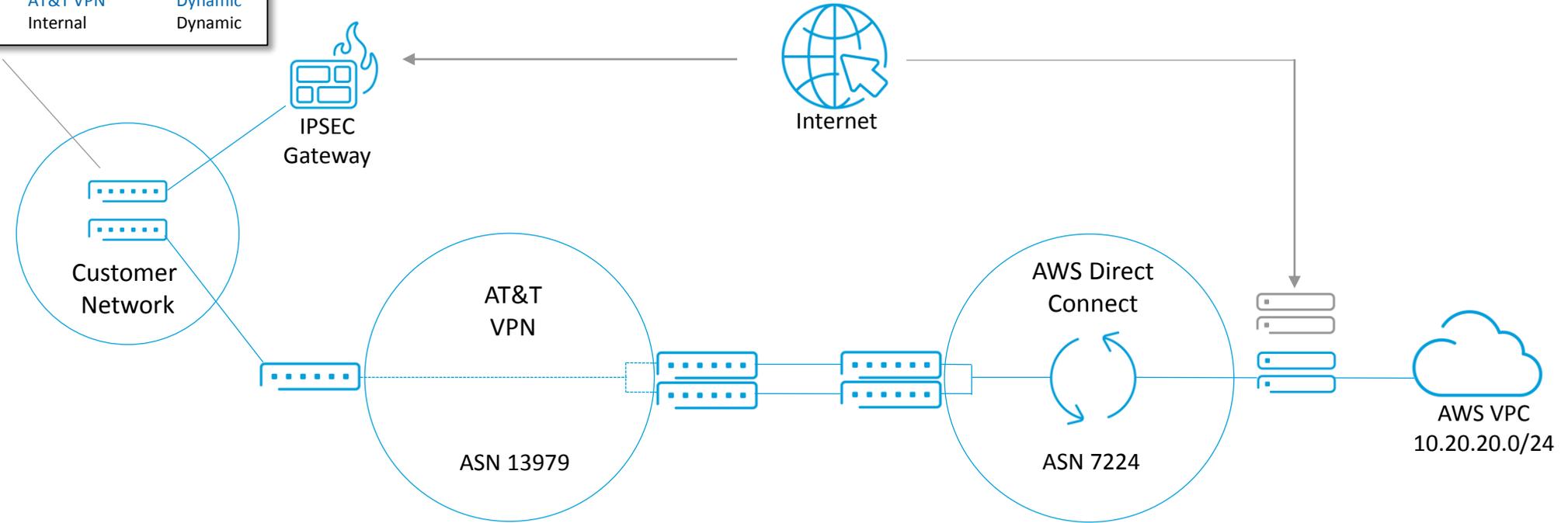
Route	Target	Routing
10.20.10.0/30	AT&T VPN	Dynamic
10.20.10.4/30	AT&T VPN	Dynamic
10.20.20.0/24	Firewall	Static
172.16.0.0/24	Internal	Dynamic



When migrating from a site-to-site VPN tunnel to NetBond, it is recommended that the NetBond connection be activated to a second VGW that has **not** yet been attached to the VPC.

Migrating from Site to Site VPN Tunnels to NetBond (cont.)

Route	Target	Routing
10.20.10.0/30	AT&T VPN	Dynamic
10.20.10.4/30	AT&T VPN	Dynamic
10.20.20.0/24	Firewall	Static
10.20.20.0/24	AT&T VPN	Dynamic
172.16.0.0/24	Internal	Dynamic



During the migration maintenance window, detach the original VGW from the VPC, and attach the new VGW. Update route tables to use the new VGW. Remove any static routes that were configured at the premise that routed traffic to AWS via the VPN gateway.

VNC Itemized Billing

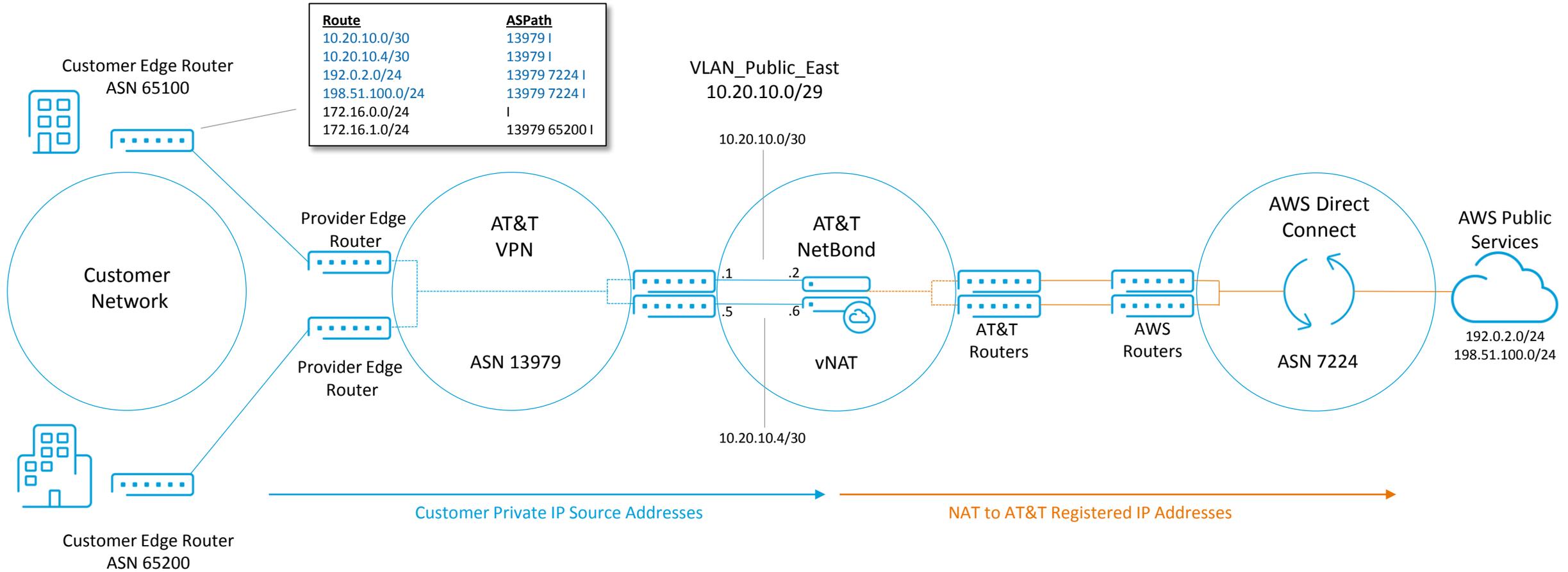
If a customer requires internal cost allocation they will need to establish individual subaccounts during initial VNC creation. This will provide itemized billing on the invoice.

Considerations

- Users that need access to all subaccounts should be configured as Enterprise Managers
- Usage Notification Alerts are per subaccount.
- Portal Reporting is per subaccount.
- NetBond features that are in controlled introduction would require an AT&T Cloud Portal trouble ticket. You will need to create the subaccount first so that AT&T can complete the service ticket request.
- Once a VNC is created under one subaccount, it cannot be migrated to another subaccount. It must be rebuilt in the new subaccount which will result in downtime.

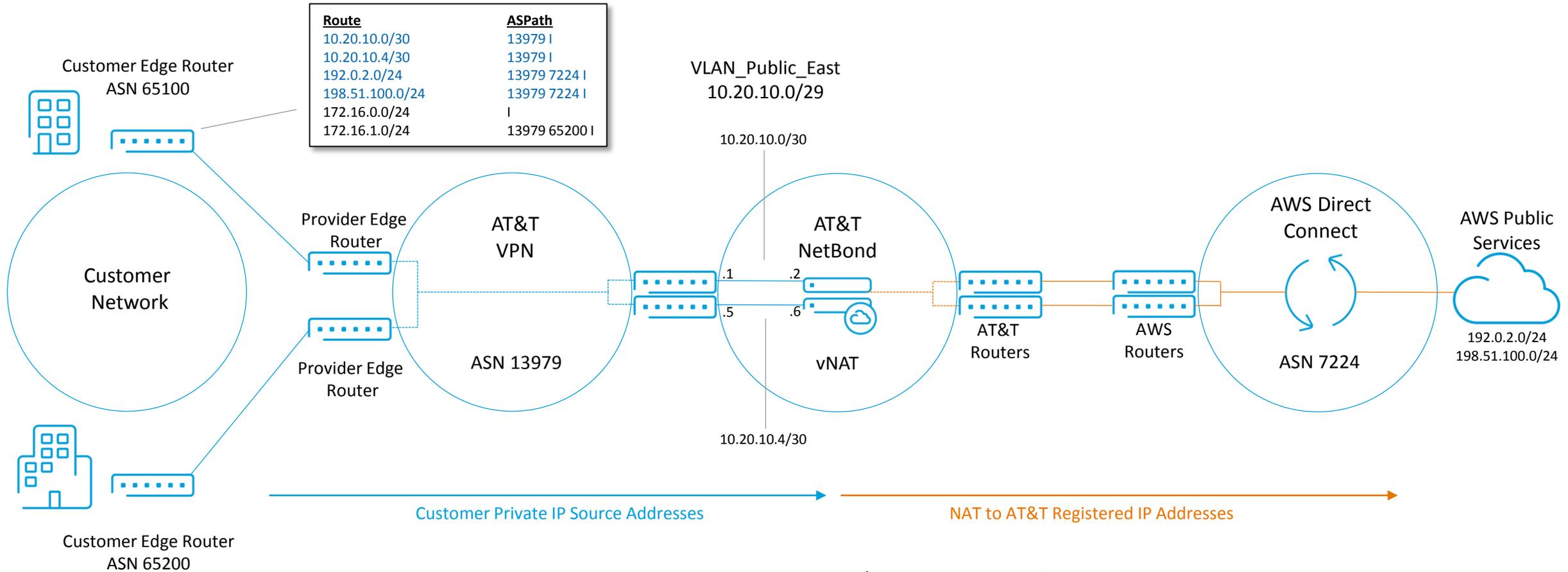
Service Activation Overview for AWS Public Services

Public Services



NetBond can also provide connectivity to AWS PaaS type services such as S3 or Route 53. Since these services run in the AWS public IP space, AT&T will provision a virtual network address translation device, (vNAT) to translate the customer's enterprise IP space to an AT&T registered public IP address. All of AWS' public routes are advertised into the customer's enterprise routing tables.

Public Services (cont.)



In our example, our customer creates a new VNC and new VLAN with a /29 address space and the AWS account number. In the AWS console, our customer accepts two new Direct Connect virtual interfaces, but no VGW is required. Instead the customer must wait for AWS to accept the AT&T public route announcements using an AT&T Letter of Authorization.

One consideration customer should take into account is that the enterprise will forward traffic for all AWS public services via NetBond. Thus, if any host on the network is conducting a transaction with a third party who happens to use AWS Public IP space as an underpinning to their website or service, then that transaction will occur over NetBond.

What's Next?

What's Next After Activation? Confirming Connectivity

1. For the first connection to AWS, schedule an activation call with the NetBond Onboarding Team.
2. After successfully creating your Virtual Network Connection (VNC) and VLAN, we want to confirm basic network connectivity to AWS.
3. After basic connectivity is confirmed, we ask that you take the following five business days to test your applications over NetBond. Our Client Technical Lead, (CTL) is available to assist during this time if you have any questions or concerns, and they can be reached at DL-NetBondTeam@att.com.
4. After five business days, our cloud support team is available 24x7 to provide technical support and answer any questions. In addition, if you run into an emergency over these next five days, please open a ticket in the Cloud Portal to engage our cloud support team.

