

AT&T NetBond[®] for Microsoft Azure[™]

Service Activation Overview

© 2017 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. Microsoft Azure marks are the trademarks and service marks of Microsoft. All other marks contained herein are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change..



AT&T NetBond allows AT&T customers to extend their MPLS virtual private network to cloud services such as Microsoft Azure. With NetBond enabled, an Azure VNet[™] or Azure public service such as blob storage will appear as another site on the VPN. Customers can then reach their virtual machines or blob storage 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 Microsoft. 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 <u>www.synaptic.att.com</u>.



Service Activation Overview for Azure VNet



Example Scenario – Customer with existing AT&T VPN and Azure VNet



Azure VNet 10.20.20.0/24

Customer Edge Router ASN 65200 172.16.1.0/24 The next few slides provide an overview of a typical service activation with an Azure VNet. In this example, our customer has a private network with AT&T VPN service, and two representative US sites using BGP local ASNs 65100 and 65200. An existing Azure VNet is ready with an IP address range of 10.20.20.0/24



© 2017 AT&T Intellectual Property. All rights reserved.

Prerequisite – Create ExpressRoute VNet Gateway





Customer Edge Router ASN 65200 172.16.1.0/24

.

Prior to NetBond service activation, within the Azure portal, our customer creates an ExpressRoute VNet gateway within the VNet. VNet gateways provide private networking connectivity for VNets. Site-to-site VPN tunnels over the Internet are also terminated on VNet gateways. The ExpressRoute VNet gateway IP space is allocated from the VNet's CIDR block and should be at a minimum a /28 address block. This process can take up to 45 minutes and must be completed prior to the scheduled service activation call.

Note: Customers wishing to maintain a site-to-site IPSEC tunnel in conjunction with NetBond/ExpressRoute connectivity should consult with their Microsoft support representative prior to performing this step.



Prerequisite #2 – Create ExpressRoute Circuit



Customer Edge Router ASN 65200 172.16.1.0/24

.

6

Additionally, prior to NetBond service activation, within the Azure portal, our customer creates an ExpressRoute circuit within a designated Microsoft peering location. "AT&T NetBond" is chosen as the service provider. A "standard" service SKU is sufficient for MPLS VPN's with less than 4,000 routes and VNets in one continent. For global VNet deployments or networks greater than 4,000 routes, a "premium" service SKU is required.

Instructions for creating an ExpressRoute circuit can be found at the following link. **Only follow steps 1-4**. <u>https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-circuit-portal-resource-manager</u> Once the ExpressRoute is created, note the associated service key in the Azure portal.



Step 1 – Create Virtual Network Connection (VNC)





Customer Edge Router ASN 65200 172.16.1.0/24 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 MPLS private network on the AT&T routers at the meet-me point with the Microsoft routers. In addition, our customer chooses a minimum bandwidth commitment for the virtual network connection.



Step 2 – Create VLAN





Customer Edge Router ASN 65200 172.16.1.0/24 Using the ExpressRoute service key 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 VNet address space. NetBond orchestration provisions a pair of connections between the virtual routing interface on the AT&T routers and the Azure ExpressRoute circuit. The /29 space is automatically provisioned as two /30 subnets.

The customer edge routers will now see the /30 subnets in their routing tables. Note the Azure VNet, (10.20.20.0/24 in the example), will not yet appear since the VNet is not connected to the ExpressRoute circuit.



Step 3 – Connect Azure VNet to ExpressRoute Circuit





Customer Edge Router ASN 65200 172.16.1.0/24 Once the NetBond orchestration is complete, the Azure administrator will notice in the Azure portal that the ExpressRoute circuit's Service Provider Status is now "Provisioned". The Azure administrator now links the VNet gateway to the ExpressRoute circuit. Instructions can be found at:

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager

After a few minutes, Azure will finish provisioning the connections to the ExpressRoute, and the CIDR block associated with the VNet will automatically be advertised to all sites on the MPLS VPN.



WARNING! Peering Status and ExpressRoute Routing Configuration

Note that Microsoft does not show BGP configuration information for Layer 3 providers such as AT&T. Per Microsoft's web site:

"We currently do not advertise peerings configured by service providers through the service management portal. We are working on enabling this capability soon."

Additionally, AT&T configures and maintains the ExpressRoute routing configuration. Do not configure any of these settings in the Azure portal.

Occasionally a Microsoft support representative may incorrectly instruct you to configure the ExpressRoute circuit's routing configuration. Under no circumstances should this be done. Instead, remind them that AT&T is a service provider providing managed Level 3 services with ExpressRoute.



Additional VNets





Customer Edge Router ASN 65200 172.16.1.0/24 In the Microsoft Azure portal, additional VNets can be linked to the same ExpressRoute. If the Azure subscription for the VNet does not match the subscription used to create the ExpressRoute, the Azure administrator must follow special steps to authorize the link using PowerShell:

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-arm

The additional VNet address space will automatically be propagated to all MPLS VPN sites upon completing the link to the ExpressRoute in the Azure portal.



Summary Steps

- 1. Obtain an Azure subscription.
- 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 Azure, at least one VNet with an attached VNet Gateway is required.
- 4. Using the Azure portal, create ExpressRoute circuit and note the service key.
- 5. Using the AT&T Cloud Services portal, create NetBond Virtual Network Connection. (Required: Name of AT&T VPN, region, free-form name for Virtual Network Connection, and minimum bandwidth commitment)
- 6. Additionally, within the AT&T Cloud Services portal, create NetBond VLAN. (Required: /29 address space, free-form name, and ExpressRoute service key)
- 7. Link VNet to ExpressRoute through the Azure portal.



Technical Considerations



Default Route



ASN 65200

172.16.1.0/24

If the default route is advertised into the MPLS VPN, and subsequently through NetBond, Microsoft Azure will prefer it over the current Azure Internet gateway. As a result, any traffic destined for the Internet will be routed back to the MPLS VPN instead of directly to the Azure Internet gateway. In some architectures, this may be the desired path for Internet traffic. In others where direct Internet access through Azure is desired, filtering the default route in the AT&T Cloud Services portal is required.



Filter Default Route with AT&T Route Management



ASN 65200 172.16.1.0/24

Using the AT&T Cloud Services portal, the NetBond administrator can choose to filter the default route advertisement to Azure. This capability is available at the VLAN level within NetBond using the route management policies and can be enabled during or after VLAN creation by clicking the appropriate radio button.



VNet Subnet Default Route Granularity with Azure Route Tables



Alternatively, if our customer's Azure administrator wants to fine tune which subnets within VNets use the Azure Internet gateway, they can utilize Azure User Defined Routes to modify the route table of a particular subnet. Any user defined route within the VNet route table will override any routes learned via ExpressRoute. More information on User Defined Routes for Azure can be found at:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

In the example above, the administrator chose to have Subnet 1 use the Azure Internet gateway by creating a user defined route for the default route with Next Hop Type of "Internet". Note: ExpressRoute cannot be designated as a "Next Hop Type". However, routes learned from ExpressRoute can be overridden with User Defined Routes configured with a target of "Internet", "Virtual Appliance", or "None".



Additional Route Management Capabilities

Through the AT&T Cloud Services portal, NetBond provides additional route policy management features. Use cases include overcoming the Microsoft route limit, (4,000 routes for standard ExpressRoute), backup VNCs for redundancy, or limiting specific routes for security purposes.

Routes advertised by AT&T to Microsoft

- Block the default route
- Limit routes advertised based on a community value applied at the customer edge routers.
- Advertise only manually specified routes
- Prepend route advertisements with extra AS hops.

Routes advertised by Microsoft to AT&T

- Block manually specified routes
- Block or Allow based on community values applied by Microsoft
- Apply manually specified community values prior to advertisement to the MPLS VPN
- Prepend route advertisements with extra AS hops
- Advertise only manually specified routes to the MPLS VPN



Migrating from Site to Site VPN Tunnels to NetBond



When migrating from a site-to-site VPN tunnel to NetBond, first establish NetBond connectivity with the ExpressRoute circuit.



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



During the migration maintenance window, delete the existing VNet gateway and attach a new VNet gateway to the VNet. (This can take up to 45 minutes to complete.) Then link the new VNet gateway to the ExpressRoute.

Remove any static routes that were configured at the premise that routed traffic to Azure 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 Azure Public Services



Public Services



Customer Edge Router ASN 65200

NetBond can also provide connectivity to Azure PaaS type services such as Blob Storage or Site Recovery. Since these services run in the Azure 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 Azure's public routes are advertised into the customer's enterprise routing tables. (Office 365 routes are not included in Public Peering)



Public Services (cont.)



Customer Edge Router ASN 65200

In our example, our customer creates a new VNC, using the "Public" routing domain. Next a VLAN is created with a new /29 address space and the ExpressRoute service key. (The same ExpressRoute used for private peering can be shared for public peering.) Microsoft has preapproved all AT&T registered public IP addresses, so connectivity will come up immediately. All Microsoft subnets used for Azure public services will be advertised to the customer's MPLS VPN.

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

T&1



What's Next?



© 2017 AT&T Intellectual Property. All rights reserved

What's Next After Activation? Confirming Connectivity

- 1. For the first connection to Azure, 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 Azure.
- 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 <u>DL-NetBondTeam@att.com</u>.
- 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.



