Lumen® SD-WAN

SD-WAN branch in Azure overview

August 2023

LUMEN®

General disclaimer

Although Lumen has attempted to provide accurate information in this guide, Lumen does not warrant or guarantee the accuracy of the information provided herein. Lumen may change the programs or products mentioned at any time without prior notice. Mention of non-Lumen products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

ALL INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED “AS IS,” WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED OR STATUTORY. LUMEN AND ITS SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES RELATED TO THIS GUIDE AND THE INFORMATION CONTAINED HEREIN, WHETHER EXPRESSED OR IMPLIED OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

LUMEN AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS OR SERVICES, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF THE GUIDE OR ANY LUMEN PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED IN THIS GUIDE, EVEN IF LUMEN OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and other information used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Many of the Lumen products and services identified in this guide are provided with, and subject to, written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this guide shall be deemed to expand, alter, or modify any warranty or license or any other agreement provided by Lumen with any Lumen product, or to create any new or additional warranties or licenses.

Overview

This document provides an overview of the steps a customer will need to perform in the customer-owned Azure environment in the support of a Lumen SD-WAN branch VM deployment. The customer will also need to provide several pieces of information back to Lumen to facilitate the deployment.

Topics covered in this document:

- Customer cloud infrastructure in Azure.
- Azure storage account and key information.
- Active Directory Application in Azure.
- Resource manager templates to simplify customer Azure setup.
- Structure for single VM or a dual VM high availability design.

Customer is required to have their own Azure infrastructure account and will have to perform all Azure steps to support the VM deployment. Customer account should have, but not limited to, a vNet with associated CIDR block, Internet gateway, security groups, and route tables. If the customer also requires Lumen MPLS connectivity, they will need to create a virtual network gateway (Express Route), attach it to the vNet.

NOTE: Lumen will be able to provide the customer with a resource manager template described below that will cover the deployment of many of these requirements.

Design topologies

Our preferred deployment approach establishes a separate vNet to host the SD-WAN VMs in the customer Azure environment. Figure 1 below shows a brief overview of each deployment.

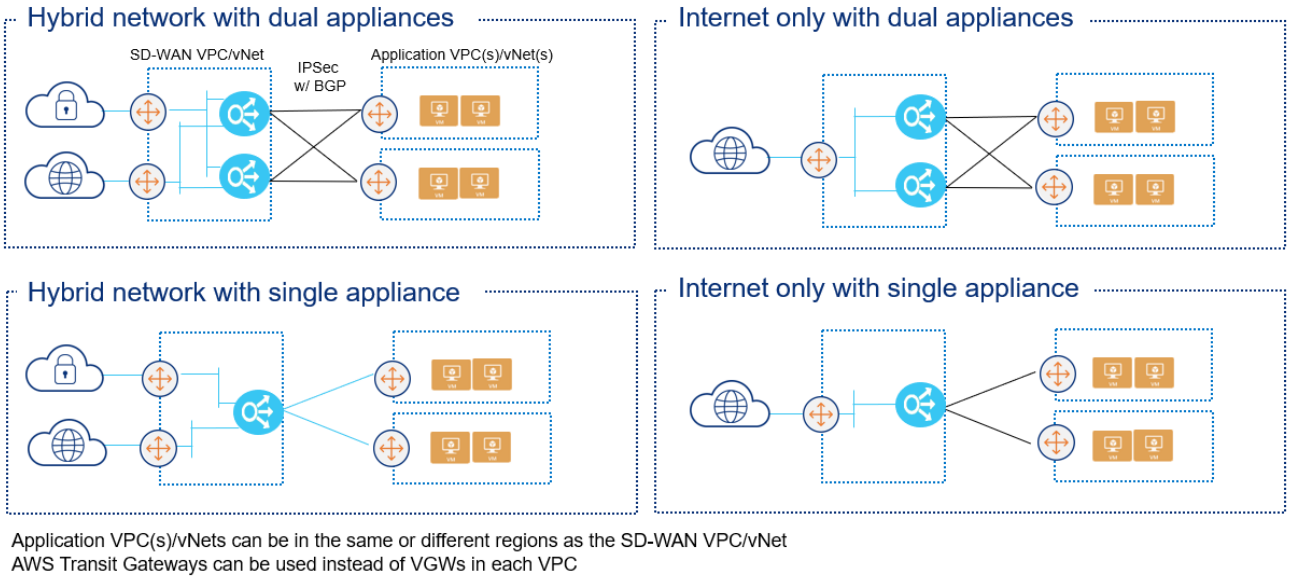

Figure 1: Cloud SD-WAN deployment topologies

Resource manager templates

Lumen can provide the customer with resource manager templates for each of the design topologies in Figure 1. These templates will create the vNet, subnets using a /24 CIDR block, associated route table, default route, and security groups to support the networks. Below is a summary of the 2 template options that the Lumen TDE can provide to the customer. These will be referred to later as a step in the process to follow.

Azure-SDWAN-HA INET.json: Creates a VNET, three subnets (MGMT, INET and LAN) using a single /24 CIDR block, associated route table, default route and three security groups to support the following deployment models:

- Single, non-HA device in a single region with Internet Overlay only
- Dual HA appliances in a single region with Internet Overlay only
- Dual HA appliances in different regions with Internet Overlay only - template will need to be deployed in each region separately

Azure-SDWAN-HA-INET-MPLS.json: Creates a VNET, four subnets (MGMT, INET, LAN and MPLS) using a single /24 CIDR block, associated route tables, routes, and security groups to support the following deployment models:

1. Single, non-HA device in a single region with Internet and MPLS Overlays

2. Dual HA appliances in a single region with Internet and MPLS overlays
3. Dual HA appliances in different regions with Internet and MPLS overlays - template will need to be deployed in each region separately and will require a virtual private gateway and ExpressRoute circuit in each region.

Once the template has been deployed, the customer will need to perform the following steps within the Azure portal or CLI. These steps are only required if MPLS connectivity is required. The virtual network gateway created in these steps is to support MPLS connectivity and do not provide IPSec connectivity from Host VNETs to the SD-WAN appliances. The steps for items 2 through 4 are covered in more detail later in the document.

1. Complete the ordering and provisioning of ExpressRoute circuits.
2. Create a virtual network gateway of the type 'ExpressRoute' and attach it to the SDWANTransitVNET.
3. Create a 'Connection' to link the ExpressRoute circuit to the virtual network gateway.
4. Create a static default route in the SdwanMPLSRouteTable with the next-hop of the Virtual network gateway (optional).

Deployment requirements and overview

Create an Azure Storage account and blob (customer)

1. Create an Azure Storage account.
2. Create a blob and add a container in the blob.
3. Navigate to Settings > Access Keys and provide either “Key1” or Key2” back to the Lumen TDE (technical design engineer).
4. Navigate to the new container and properties and provide the URL listed to the Lumen TDE.
5. Lumen TDE will then request Versa to load the proper VM image file into the container provided. Please allow 2 business days for the file to be loaded.
6. Once notified by Lumen TDE, customer will be required to “Create Image” in the Azure account. The loaded file will be utilized to create this VM image.

Create an Azure active directory application (customer)

1. Customer must create an Azure active directory application. To perform this step in Azure, administrator level access is required.
2. Select Azure Active Directory > App registrations > Add.
3. Follow these steps in the Create window:
    a. Specify a name and URL for the application. Ex. “example-app”
    b. Select Web/API for the type of application.
    c. Click Create.
4. This successfully creates and Azure active directory application.
5. Assign the application to a role.
    a. Navigate to All Services > Subscriptions.
    b. Select the subscription to assign the application to.
    c. Select Access Control (IAM).
    d. Select Add role assignment.
    e. To allow the application to execute actions like reboot, start, and stop, select the Contributor role.
    f. Find the newly created app from the steps above and select it in the “Select” menu.
    g. Select Save to finish assigning the role.
6. The following information will need to be retrieved and provided back to Lumen TDE.

a. Application ID – Select your application from app registrations in Azure active directory. Copy the application ID and save it to provide to Lumen TDE.

b. Certificate and Secrets – Select Certificates and Secrets > Select Client Secrets > New client secret. Provide a description for the secret and a duration (expires in 1 year is recommended). The value will be generated when clicking Save.

   NOTE: Please make sure to copy this key at this time. It cannot be retrieved again after navigating away from this screen.

c. Directory ID – Select properties for your Azure tenant and copy the directory ID.

d. Subscription ID – Navigate to the Overview tab on the Azure account and copy the subscription ID.

For additional information on this part of the process, please also reference MS Azure article at: Azure - Create Service Principal Portal

Overview of Lumen deployment steps

- Lumen TDE will ensure the correct version of the FlexVNF image is loaded in the customer Azure account.
- Lumen will create a CMS connector to the customer Azure environment to support deployment of the Versa VMs.
- Lumen will continue with completing the deployment templates to build and support the activation of the VM(s).

VM sizing

The following table represents the VM sizes that are available and are standard Azure VM sizes. The size of the VM chosen should be based on the desired throughput and interfaces required.

NOTE: Lumen recommends the use of the Standard_F4s due to the similar throughput numbers and requirement for 3 NICs for the minimum design. Use of the larger VMs will drive additional cost to the customer's Azure account.

NOTE: Azure Accelerated Networking is not supported on the current release of FlexVNF running Ubuntu 14.x. It is recommended that the small VM be used and the medium and large VMs not be used to prevent incurring unnecessary charges. Versa projects that throughput size limitations can be overcome as part of Versa 22.1, which is supposed to have an Azure-compliant version of DPDK.

Azure								
vCPE Size	Throughput BW	Cores	RAM	Disk	NICs	VM NIC Type	CPU Type	Cloud Provider Designation
Small-FlexVNF	187 Mbps	4	8G	16G	4	1 or 2	Intel Sandy or better	Standard_F4s
Medium-FlexVNF	157 Mbps	8	16G	32G	8	1 or 2	Intel Sandy or better	Standard_F8s
Large-FlexVNF	178 Mbps	16	32G	64G	8	1 or 2	Intel Sandy or better	Standard_F16s

Internet-only deployments

In these designs, the customer only requires internet WAN connectivity into their cloud environment. Figure 2 below shows an overview of the single VM or dual VM deployment topologies.

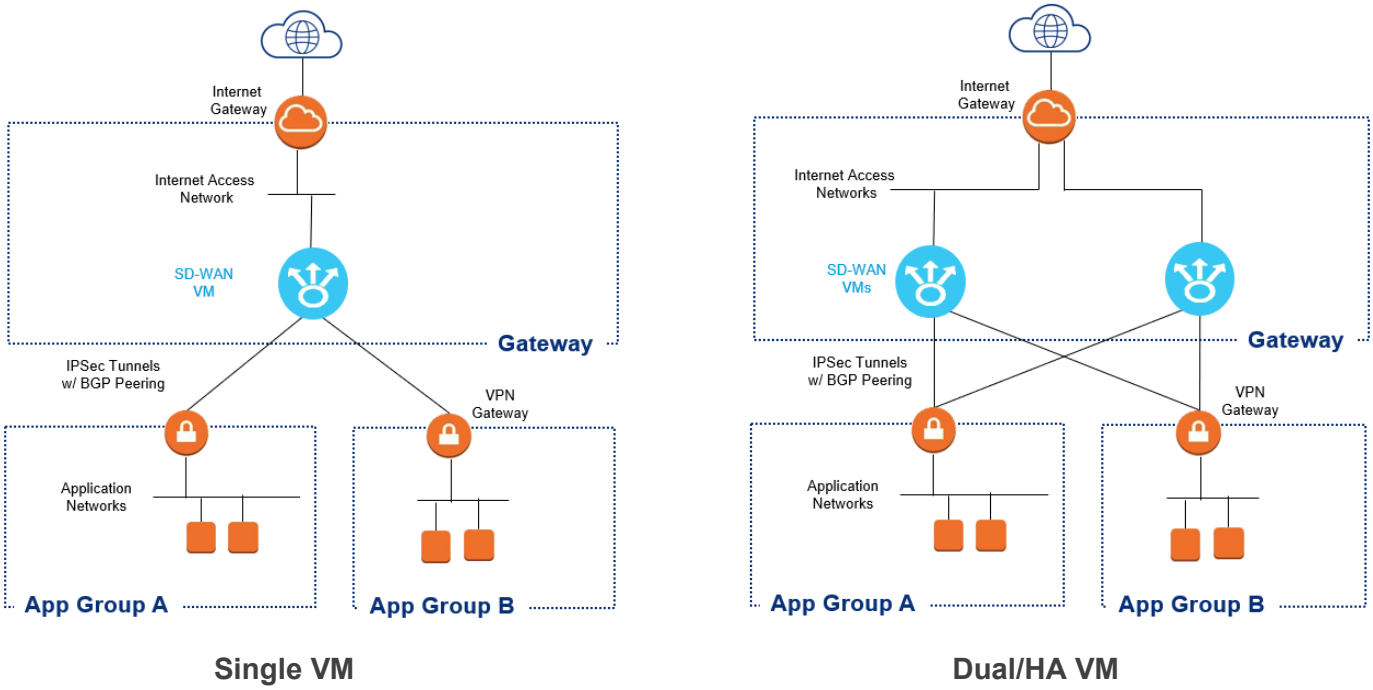

Figure 2

Summary of customer steps for deployment

For the internet-only deployment topologies, below is a summary of the steps required by the customer to complete this configuration/deployment.

1. Request the appropriate resource manager template from the Lumen TDE and run them in the customer Azure environment. Please use the internet only template for this deployment type. Template will need run twice if deploying dual VMs in different regions.

   NOTE: Gateway vNet requirements are also covered in the appendix of this document for reference and many of these steps are part of the resource manager templates.

2. HOLD step – Customer will wait until Lumen has deployed the SD-WAN VM instances to proceed further. Steps are listed above in the overview of Lumen deployment steps.

3. Create local network gateways - This step defines the SD-WAN appliances as customer VPN gateways that can be used by the VNGW.

   a. Navigate to 'Local Network Gateways' and click the '+' to add a local gateway.

b. Provide a unique name, public IP assigned to the SD-WAN appliance, the IP subnet in slash notation of the LAN port of the SD-WAN appliance, check 'Configure BGP', enter the AS number used in the LAN-VR of the SD-WAN appliance (64514 by default), enter the LAN IP address of the SD-WAN appliance and select the appropriate resource group.

c. Click 'Create' to start the deployment process.

d. Repeat the above steps for the second SD-WAN appliance.

4. Create VNGW - the customer must create a VNGW in each Host VNET that will use the SD-WAN appliances.

   a. Navigate to the 'Virtual Network Gateways' blade and click the '+' to create a new VNGW.

   b. Provide a name, select a region, select 'VPN' as the gateway type, select 'Route-based' for VPN type, select the appropriate SKU (do not use Basic) and select the appropriate Host VNET from the list.

   c. For active-backup mode, create a new IP and provide a name, leave 'Enable active-active mode' set to disabled, enable 'Configure BGP ASN' and enter the AS number that will be assigned to the VNGW. This will be used as the peer-as in the SD-WAN appliances.

   d. For active-active mode, create a new IP and provide a name, enable 'Enable active-active mode', create a new, second public IP and provide a name, enable 'Configure BGP ASN' and enter the AS number that will be assigned to the VNGW. This will be used as the peer-as in the SD-WAN appliances.

   e. Click 'Review + Create', which will run a validation and then click 'Create' to begin the VNGW deployment. This process can take considerable time (Azure advises up to 45 minutes).

   Note: This step creates a 'GatewaySubnet' in the Host VNET that is used to associate the VNGW, BGP sessions and routes to. This subnet will use the next available IP range out of the CIDR for the VNET.

5. Create connections - this step will create the IPSec connections and BGP sessions between the VNGW and SD-WAN appliances.

   a. Navigate to 'Virtual Network Gateways' and select the VNGW created in the last step.

   b. Select 'Configuration' and ensure the VNGW is in the correct mode. Ensure the correct BGP ASN is configured and make a note of the BGP Peer IP Address(s). This information will be required to configure the SD-WAN appliances and will need to be provided to Lumen personnel.

   c. Select 'Connections' and then click the '+' to add a connection.

   d. Provide a unique name, select 'Site-to-Site (IPSec)' for the connection type, select a local network gateway from the dropdown, enter a pre-shared key and click 'OK' to create the connection. The pre-shared for each connection is required to configure the SD-WAN appliances and will need to be provided to Lumen personnel.

e. Once created, navigate back to 'Virtual Network Gateways', select 'Connections', click on the connection you just added, click 'Configuration' and ensure BGP is enabled. If this changes, click 'Save' at the top of the blade.

f. Repeat the above steps to create the connection(s) to the second SD-WAN appliance.

Note: If the customer has additional host VNETs that will use the SD-WAN appliances, the above steps will need to be repeated for each host VNET. A maximum of five host VNETs can be supported by a pair of SD-WAN appliances due to limitations with the allowed number of WAN based IPSec tunnels. Only ten WAN-based IPSec tunnels are allowed per appliance and with the VNGWs in active-active mode with two IPSec tunnels active, that allows for five host VNETs.

Hybrid deployments with MPLS

In these designs, the customer requires both Internet and MPLS connectivity into their cloud environment. Figure 3 below shows an overview of the single VM or dual VM deployment topologies.

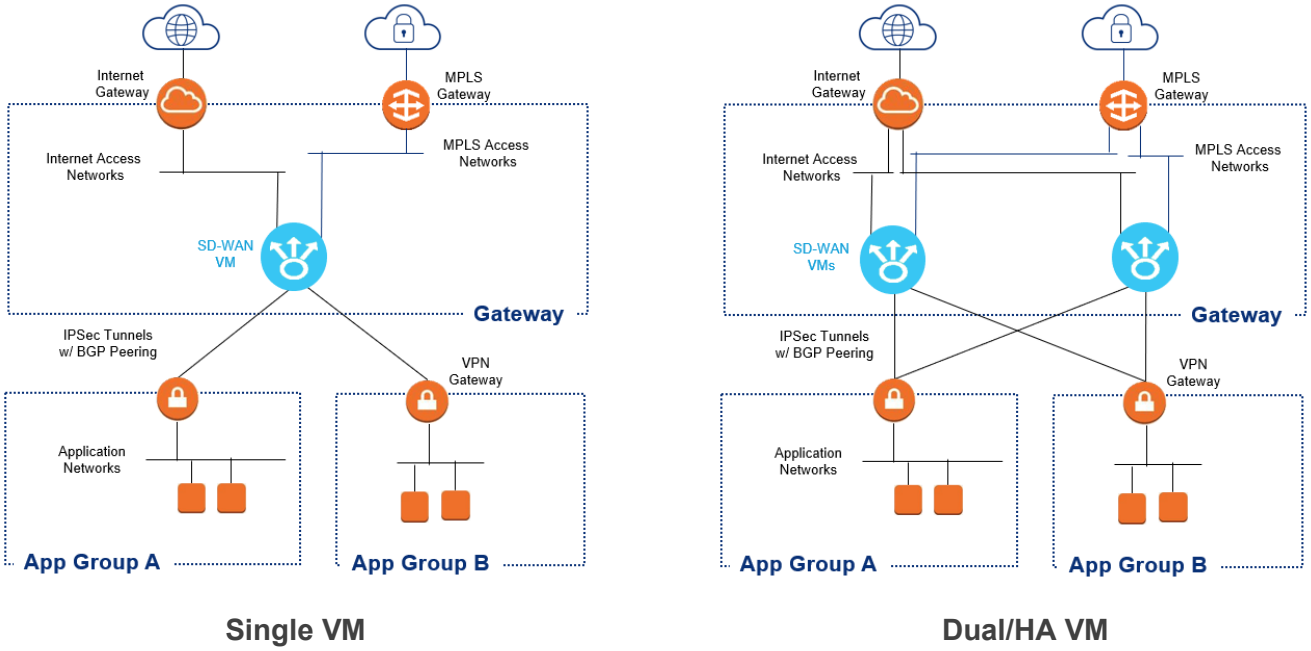

Figure 3

Summary of customer steps for deployment

Like the internet only deployment topologies, the customer will need to do many of the same steps and additional steps related to setting up and attaching the MPLS/VPN connection. Below is a summary of the steps required by the customer to complete this configuration/deployment.

1. Request the appropriate resource manager template from the Lumen TDE and run them in the customer Azure environment. Please use the “INET-MPLS” template for this deployment type. Template will need run twice if deploying dual VMs in different regions.

NOTE: Gateway VNET requirements are also covered in the appendix of this document for reference and many of these steps are part of the resource manager templates.

1. HOLD step – Customer will wait until Lumen has deployed the SD-WAN VM instances to proceed further. Steps are listed above in the overview of Lumen deployment steps.
2. Create local network gateways - This step defines the SD-WAN appliances as customer VPN gateways that can be used by the VNGW.
    a. Navigate to 'Local Network Gateways' and click the '+' to add a local gateway.

b. Provide a unique name, public IP assigned to the SD-WAN appliance, the IP subnet in slash notation of the LAN port of the SD-WAN appliance, check 'Configure BGP', enter the AS number used in the LAN-VR of the SD-WAN appliance (64514 by default), enter the LAN IP address of the SD-WAN appliance and select the appropriate resource group.

c. Click 'Create' to start the deployment process.

d. Repeat the above steps for the second SD-WAN appliance.

3. Create VNGW - the customer must create a VNGW in each host VNET that will use the SD-WAN appliances.

   a. Navigate to the 'Virtual Network Gateways' blade and click the '+' to create a new VNGW.

   b. Provide a name, select a region, select 'VPN' as the gateway type, select 'Route-based' for VPN type, select the appropriate SKU (do not use Basic) and select the appropriate Host VNET from the list.

   c. For active-backup mode, create a new IP and provide a name, leave 'Enable active-active mode' set to disabled, enable 'Configure BGP ASN' and enter the AS number that will be assigned to the VNGW. This will be used as the peer-as in the SD-WAN appliances.

   d. For active-active mode, create a new IP and provide a name, enable 'Enable active-active mode', create a new, second public IP and provide a name, enable 'Configure BGP ASN' and enter the AS number that will be assigned to the VNGW. This will be used as the peer-as in the SD-WAN appliances.

   e. Click 'Review + Create', which will run a validation and then click 'Create' to begin the VNGW deployment. This process can take considerable time (Azure advises up to 45 minutes).

   Note: This step creates a 'GatewaySubnet' in the host VNET that is used to associate the VNGW, BGP sessions and routes to. This subnet will use the next available IP range out of the CIDR for the VNET.

4. Create connections - this step will create the IPSec connections and BGP sessions between the VNGW and SD-WAN appliances.

   a. Navigate to 'Virtual Network Gateways' and select the VNGW created in the last step.

   b. Select 'Configuration' and ensure the VNGW is in the correct mode. Ensure the correct BGP ASN is configured and make a note of the BGP peer IP address(s). This information will be required to configure the SD-WAN Appliances and will need to be provided to Lumen personnel.

   c. Select 'Connections' and then click the '+' to add a connection.

   d. Provide a unique name, select 'Site-to-Site (IPSec)' for the connection type, select a local network gateway from the list, enter a pre-shared key and click 'OK' to create the connection. The pre-shared for each connection is required to configure the SD-WAN appliances and will need to be provided to Lumen personnel.

e. Once created, navigate back to 'Virtual Network Gateways', select 'Connections', click on the connection you just added, click 'Configuration' and ensure BGP is enabled. If this changes, click 'Save' at the top of the blade.

f. Repeat the above steps to create the connection(s) to the second SD-WAN appliance.

Note: If the customer has additional host VNETs that will use the SD-WAN appliances, the above steps will need to be repeated for each host VNET. A maximum of five host VNETs can be supported by a pair of SD-WAN appliances due to limitations with the allowed number of WAN-based IPSec tunnels. Only ten WAN-based IPSec tunnels are allowed per appliance and with the VNGWs in active-active mode with two IPSec tunnels active, that allows for five Host VNETs.

Additional customer steps in Azure for MPLS connectivity

Connectivity between a customer's Azure infrastructure and an MPLS service is supported. The following addendum details requirements and steps to connect to a Lumen service such as Lumen® Cloud Connect or VPNLynk. Azure refers to this connectivity as ExpressRoute. Within the ExpressRoute product suite is an any-to-any connection method, which will connect the customer's Azure network to a provider's MPLS cloud. By default, this connection is available to all Azure regions within a geo-political region. The premium service allows this connection to be available globally. The following steps must be completed by the customer in the Azure portal:

1. To support native controller access on legacy Level 3 MPLS services, the customer will need to add the above provided /29 IP block from the 100.88.0.0/23 range as a secondary CIDR in the VNET.
2. Customer must have a VNET with an associated CIDR block, four subnets, security groups for the management and Internet WAN subnets and route tables associated to each subnet. The customer must use the above /29 block from the 100.88.0.0/23 range as the IP range for the MPLS subnet connecting to the MPLS interface of the SD-WAN appliance(s).
3. Customer must create an ExpressRoute service and provide the service key to Lumen to be included in the Cloud Connect or VPNLynk service. This key will tie the Lumen service to the customer's Azure account and ExpressRoute circuit. See Azure Portal ExpressRoute How-To for further details.
4. Once the status of the ExpressRoute circuit has changed to 'provisioned', configure Azure Private Peering using the information provided by Lumen. This will include peer ASN, primary and secondary subnets, VLAN ID and a shared key for two BGP sessions. See | Azure ExpressRoute Routing How-To for further details.
5. Create a virtual network gateway of type 'ExpressRoute' and attach to the VNET. Creation of the gateway will create a gateway subnet within the VNET. See Azure ExpressRoute Gateway How-To for further details.
6. Link the ExpressRoute circuit to the newly created Gateway in the 'Connections' blade of the ExpressRoute Circuit. See Azure ExpressRoute Link To VNET How-To for further details.

7. (Optional) Create a default route in the route table attached to the MPLS subnet with a next hop type of virtual gateway. This will route all traffic in this subnet to the gateway subnet and out to the MPLS service and will allow access to resources on the MPLS network that are not advertised to Azure.

Common deployment elements

Reference: Azure virtual network gateway modes

An Azure VNET only allows communication between resources deployed within the VNET. To facilitate communication from resources within a VNET to an MPLS network or other VNETs, a gateway must be deployed and attached to the VNET. There is no internet gateway in Azure. Internet reachability is established by creating a default route in the subnet route tables with a next-hop of the Internet. Azure supports three primary gateway types:

- Virtual network gateway (VNGW) - this gateway can be configured in one of two ways. When configured in VPN Gateway mode, it allows for connectivity to other VNGWs configured as VPN gateways to allow for VNET-to-VNET connectivity or remote customer gateways to provide remote site connectivity using IPSec tunnels. A VNGW configured as a VPN gateway is required to support IPSec connectivity to FlexVNF appliances deployed in Azure. When configured in ExpressRoute gateway mode, it is used connect to ExpressRoute circuits that provide connectivity to an MPLS network. A VNGW configured as an ExpressRoute gateway is required to provide FlexVNF connectivity to a customer's MPLS network. A VNGW can only be attached to a single VNET and only one VNGW can be attached to the VNET. You cannot attach multiple VNGWs to a VNET even if they are configured in different modes. The VNGWs are deployed in pairs and can be configured in the following two modes, both modes support ECMP:
    - Active-backup - in this mode, one gateway in the pair is active and the other is backup. A single IPSec tunnel and a single BGP session is configured on each SD-WAN appliance. In the event of a VNGW member failure, the secondary VNGW member in the pair takes over the public IP, IPSec tunnel and BGP session from the first. There is an interruption in traffic flow of approximately 10–15 seconds for planned maintenance and up to 90 seconds for unplanned events (per Azure documentation).
    - Active-active - in this mode, both gateways in the pair are active. An IPSec tunnel and BGP session for each VNGW is configured on each SD-WAN appliance. A failure in one VNGW member in the pair automatically switches the traffic to the other member of the pair. Minimal traffic loss may occur.

  Note: IPSec tunnels are created between the VNGW and the SD-WAN appliances using the public internet WAN IP of each appliance. Additional per-GB charges will apply for traffic egressing the internet WAN of the appliances toward the VNGW and on to the host VNETs.

- VWAN gateway - this gateway can be attached to multiple VNETs allowing for connectivity between VNETs and can also be used as an IPSec gateway for connectivity to remote gateways. It also supports connections to ExpressRoute circuits and can provide connectivity to an MPLS network. Within a VWAN gateway, hubs are created that represent a route table and VNETs are attached to the hub. This allows for a single VWAN gateway to be used while maintaining route separation between VNETs or remote IPSec gateways. No other gateway type can be attached to a VNET when a VWAN gateway is attached and a

VNET can only be attached to a single hub. Use of a VWAN gateway requires a VPN gateway to be configured to handle the IPSec tunnels.

- Virtual route server - this gateway is deployed directly in a VNET and provides the ability to learn routes from third-party virtual routing devices via BGP to support an HA deployment model. This gateway does not provide any connectivity outside of the VNET and any routes learned via BGP are not redistributed to other VNETs when using VNET peering or VNGW-to-VNGW peering. This gateway type is not supported for FlexVNF cloud deployments.

Azure also supports VNET-to-VNET peering which allows communication between VNETs without the use of VNGWs. Peering of this type does not apply to FlexVNF cloud deployments as IPSec tunnels are used to establish reachability to host VNETs instead of attaching a gateway. The only gateway attached to the transit VNET is a VNGW configured in ExpressRoute mode to support MPLS connectivity.

Reference: Gateway VNET requirements

The customer will need to create the 'Gateway VNET' within their Azure account. The standard CMS deployment methodology described in the Azure Hosted vBranch section will be used to deploy the two SD-WAN appliances in the customer's Azure infrastructure. At this time, the CMS connector doesn't support the use of availability zones or availability sets, so there is no guarantee the SD-WAN appliances will be deployed in the Azure infrastructure in a fault tolerant configuration. Azure does employ several methods to reduce the impact of planned and unplanned maintenance activities (See the Azure Managing VM Availability document for details). The only method currently available to ensure the appliances are created in a fault tolerant mode is to deploy each appliance in a different Azure region. The SD-WAN appliances should be deployed in an active-backup mode with the primary appliance residing in the region closest to the Host VNETs to prevent variations in latency between flows. The customer must complete the following steps to create the gateway VNET:

1. Create a new VNET and assign a CIDR block unique within the customer network.
2. Create a route table with a default route with the next hop set for internet for the management and internet WAN subnets.
3. Create a route table with no routes for the MPLS subnet.
4. Create a management subnet in the VNET and associate the route table with the default internet route to it.
5. Create a Internet WAN subnet in the VNET and associate the route table with the default internet route to it.
6. Create a LAN subnet in the VNET.
7. Optional if MPLS connected - Create an MPLS subnet in the VNET and associate the route table with the no route to it.
8. Create and attach a VNGW in ExpressRoute mode and enable route propagation as detailed in the **Additional customer steps in Azure for MPLS connectivity** section of this document.
9. Create a security group for management traffic per the **Subnets and security groups** section of this document.

10. Create a security group for Internet WAN traffic per the **Subnets and security groups** section of this document.
11. Create a security group for LAN traffic as per the **Subnets and security groups** section of this document.

Appendix

Appliance console configuration (optional)

Management access to the appliance can be through the Azure Cloud Serial Console available in the customer's Azure portal. **This access would be available to the customer only and Lumen personnel would not be able to use it.** This step is optional if the customer requires this access. To enable the console port on the FlexVNF appliance, complete the following steps after creating the Workflow Template.

Steps (Lumen engineer)

1. Navigate to the 'Configuration' tab, select the Templates > Device Templates tab, select the organization in the left pane and click on the device template.
2. Select the 'Others' tab in the left pane, expand 'System' and click 'Configuration'. Scroll down to the 'Console' pane and click the edit icon.
3. Check the 'Enable' box and enter an idle timeout (in seconds). Recommended setting is 600 seconds.
4. Click 'OK' to save the changes.

Customer step

1. Azure Console must be activated in the customer's Azure portal by enabling 'Boot Diagnostics' on the VM once it is running. Refer to the Azure enable serial console document for instruction on enabling and accessing Azure Serial Console once the device has been successfully instantiated.

Lumen engineer

1. Once the device template has been created/modified, create a device group to support Azure deployed devices and add the template to this device group.

Subnets and security groups

These are listed for reference but should be created using the Cloud Formation Templates.

Azure WAN security group configuration

Customer will be required to create and provide the name of a security group to be used for the WAN Interface. The security group must allow the following inbound connectivity at a minimum. The following rules must have a priority higher than the default reject rule.

Azure Internet Security Group Configuration				
Protocol	**Source IP**	**Source Port**	**Destination IP**	**Destination Port**
UDP	Any	Any	Any	4790
UDP	Any	Any	Any	4500
UDP	Any	Any	Any	500
ICMP*	Any	Any	Any	Any

Azure management security group configuration

Customer will be required to create and provide the name of a security group to be used for the MGMT Interface. The security group must allow the following inbound connectivity at a minimum. The following rules must have a priority higher than the default reject rule.

Azure MGMT Security Group Configuration				
Protocol	**Source IP**	**Source Port**	**Destination IP**	**Destination Port**
TCP	Any	Any	Any	22
TCP	Any	Any	Any	2022
ICMP*	Any	Any	Any	Any