Reading :

* [Azure compute](https://azure.microsoft.com/product-categories/compute) https://azure.microsoft.com/en-us/products/category/compute/
* [Windows virtual machines in Azure](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/) https://learn.microsoft.com/en-us/azure/virtual-machines/
* [Linux virtual machines in Azure](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/) https://learn.microsoft.com/en-us/azure/virtual-machines/
* [Azure App Service documentation](https://docs.microsoft.com/en-us/azure/app-service/) https://learn.microsoft.com/en-us/azure/app-service/
* [Azure Container Instances](https://azure.microsoft.com/services/container-instances) https://azure.microsoft.com/en-us/products/container-instances/
* [Azure Kubernetes Service](https://azure.microsoft.com/services/kubernetes-service) https://azure.microsoft.com/en-us/products/kubernetes-service/
* [Azure Functions documentation](https://docs.microsoft.com/en-us/azure/azure-functions/) https://learn.microsoft.com/en-us/azure/azure-functions/
* [Windows Virtual Desktop documentation](https://docs.microsoft.com/en-us/azure/virtual-desktop/) https://learn.microsoft.com/en-us/azure/virtual-desktop/
* [Virtual Machines documentation](https://docs.microsoft.com/en-us/azure/virtual-machines/) https://learn.microsoft.com/en-us/azure/virtual-machines/

1. Migrate database workloads to Azure, Azure SQL database (MySQL & PostgreSQL) migrate to existing SQL Server,
2. Azure Cosmos DB works with a variety of pupular APIs, including SQL, MongoDB, Cassandra, tables and Grammar. You can migrate your data to cloud
3. Big data analysis services like Azure synapse Analytics, Azure HDInsight, Azure Data breaks, and Azure Data Lake Analytics to analyze large volumes of data.
4. Challanges application demand using Azure Virtualization services like Azure Virtual Machines(AVM) , Azure Container Instances (ACI) and Azure Kubernetes Service (AKS)
5. Azure App service to create your website front-ends, Azure functions to create event-driven application logic that only runs when you need us.
6. Windows Virtual Desktop to quickly provide a customized operating system and software environment for your remote workers.

LEARN Azure Storage options, :

* Azure Blob storage
* Azure Disk storage
* Azure Files storage
* Azure Blob Access Tiers.

**Case :**

Company has a lot of product brochures like data-sheets, product images, and other files that are related  to marketing, sales, and support. In the past, your company has been hosting these files on standalone web servers in your data center. Tailwind is now in the process of migrating it's applications to the Cloud. our development team is currently architecting new applications.  Your Chief Technology Officer wants to migrate all of your marketing, sales, and support files to the Cloud, in order to take advantage of geographic distribution of your files. This move also reduces the number of physical servers that your company maintains in your data center. **As part of your migration strategy, you need to determine the correct approach for your cloud-based storage infrastructure.**

Your team has **chosen Azure Storage**, which is a service that you can use to store files, messages, tables, and other types of information. Clients such as websites, mobile apps, desktop applications, and many other types of custom solutions, can read data from and write data to Azure Storage. **Azure storage (IaaS) is also used by Infrastructure as a Service Virtual Machines and Platform as a Service (PaaS) Client Services**.

To begin using Azure Storage, you first create an Azure Storage account to store your data objects. You can create an Azure Storage account by using the Azure portal, PowerShell or the Azure CLI. You should note that **Azure Storage is not the same as Azure Database Services**. Your storage account will contain all of your Azure Storage data objects such as blobs, files and disks. For example, by using storage accounts to store her files in the cloud, Sally will be able to access these files through unique namespace, using HTTP or HTTPS. These files will be highly available and securely stored within this Azure Storage account. **Please note that Azure VMs, you use Azure Disk Storage to store virtual disks. However, you can't use Azure Disk Storage to store a disk outside of a virtual machine**. A Storage account provides a unique namespace for your Azure storage data, that's accessible from anywhere in the world over HTTP or HTTPS. Data in this account is secure, highly available, durable, and massively scalable. For more information, you can refer to the Microsoft Azure product documentation on how to create a storage account.

**Disk Storage Fundamentals :**

**Disk storage provides disks for Azure Virtual Machines**. Applications and other services can access and use these disks as needed, similar to how they would in on-premises scenarios. **Disk storage allows data to be persistently stored and accessed from an attached virtual hard disk.** Disks come in many different sizes and performance levels, from solid-state drives, SSDs, to traditional spinning hard disk drives, HDDs, with varying performance tiers. You can use standard SSD and HDD disks for less critical workloads. Premium SSD disks for mission-critical production applications, and ultra disks for data-intensive workloads such as SAP HANA, top-tier Databases, and transaction-heavy workloads. Azure has consistently delivered enterprise-grade durability fo**r Infrastructure as a service (IaaS**) disks, with an industry-leading zero percent annualized failure rate. **An Azure Virtual Machine can use separate disks to store different data.**

**Azure Blob Storage Fundamentals :**

**Azure Blob Storage is an object storage solution for the Cloud. It can store massive amounts of data, such as text or binary data. Azure Blob Storage is unstructured, meaning that there are no restrictions on the kinds of data it can hold.** Blob Storage can manage a thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an Internet connection. *Blobs aren't limited to common file formats. A blob could contain gigabytes of binary data streamed from a scientific instrument, an encrypted message for another application, or data in a custom format for an app you're developing*. **One advantage of Blob Storage over Disk Storage is that it does not require developers to think about or managed disks. Data is uploaded as blobs and Azure takes care of the physical storage needs**. Blob Storage is :

1. Ideal for storing up to eight terabytes of data for virtual machines,
2. Storing data for analysis by an on-premises or Azure hosted service,
3. Storing data for backup and restore, disaster recovery, and archiving.
4. Streaming video and audio,
5. Storing files for distributed access,
6. Serving images or documents directly to a browser.

**This diagram illustrates how you might use  Azure accounts, containers, and blobs.**

A diagram of a container

Description automatically generated

**Azure Files Fundamentals** :

**Azure Files offers fully managed file shares in the Cloud that are accessible via the industry standard server message block and network file system preview protocols.** Azure file shares can be mounted concurrently by Cloud or on-premises deployments of Windows, Linux, and macOS. **Applications running in Azure Virtual Machines or Cloud services can mount a file storage share to access file data just as a desktop application would mount, a typical SMB – Server message Block- share.** Any number of Azure Virtual Machines or roles can mount and access the file storage share simultaneously. Typical usage scenarios would be to share files anywhere in the world, diagnostic data or application data sharing. Use Azure Files for the following situations;

* **many on-premises applications use file shares.** Azure Files makes it easier to migrate those applications that share data to Azure. If you mount the Azure File share to the same drive letter that the on-premises application uses, the part of your application that accesses the file share should work with a minimal if any changes.  *Azure Files makes it easier to migrate those applications that share data to Azure.*
* **Access from multiple VMs.** Store configuration files on a file share and access them for multiple VMs. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them and that they use the same version.  *Configuration files can be stored on a file share and accessed from multiple VM. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them and that they use the same version.*
* **Later data processing and analysis.** Write data to a file share and process or analyze the data later. For example, you might want to do this with diagnostic logs, metrics and crashed dumps. *This is typically done with diagnostic logs, metrics, and crash dumps.*

A diagram of a file sharing system

Description automatically generated This illustration shows Azure Files being used to share data **between two geographical locations**. Azure Files ensures the data is encrypted at rest, and the server message block (SMB) protocol ensures that the data is encrypted in transit. One thing that distinguishes Azure Files from files on a corporate file share is that you can access the files from anywhere in the world *by using a URL that points to the file*. You can also use shared access signature (SAS) tokens to allow access to a private asset for a specific amount of time. A service SAS URI will show the resource URI and the SAS token.

A blue background with white text

Description automatically generated

**Understanding Blob Access tiers :**

Data stored in the cloud can grow at an exponential pace.  **To manage costs for your expanding storage needs, it's helpful to organize your data based on attributes like frequency of access and planned retention period**. Data stored in the cloud can be different based on how it's generated, processed and accessed over its lifetime. Some data is actively accessed and modified throughout its lifetime. Some data is accessed frequently early in its lifetime, with access dropping drastically as the data ages. Some data remains idle in the cloud and is rarely if ever accessed after it's stored.

To accommodate these different access needs, ***Azure provides several access tiers, which you can use to balance your storage costs with your access needs.***  Azure storage offers different access tiers for your blob storage, helping you store object data in the most cost effective manner.

* **Hot access tier**, optimized for storing data that is accessed frequently, for example, images for your website
* **Cool access tier,** optimized for data that is infrequently accessed and stored for at least 30 days, for example, invoices for your customers.
* **Archieve access tier,** appropriate for data that is rarely accessed and stored for at least 180 days with flexible latency requirements, for example, long term backups

Additionally, some considerations apply to the different access tiers :

* **Only the hot and cool access tiers can be set at the account level**. The archive access tier isn't available at the account level.
* **Hot, cool and archive tiers can be set up at the blob level** during upload or after upload.
* **Data in the cool access tier can tolerate slightly lower availability**, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service level agreement and higher access costs compared to hot data are acceptable tradeoffs for lower storage costs.
* **Archive storage stores data offline and offers the lowest storage costs**, but also the highest cost to rehydrate and access data.

A screenshot of a computer

Description automatically generated

This illustration demonstrates choosing between the hot and cool access tiers on a general purpose storage account.

A close-up of a computer screen

Description automatically generated A screenshot of a computer

Description automatically generated

A close-up of a message

Description automatically generated A close-up of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

**Different Azure Networking Options**.

Case: A Company has on-premises data center that you plan to keep, but you want to use Azure to offload peak traffic by using virtual machines hosted in Azure. You want to keep your existing IP addressing scheme, and network appliances while ensuring that any data transfer is secure. Using Azure Virtual Network for your virtual networking can help you reach your goals. **Azure virtual networks enable Azure resources such as VMs, web apps, and databases, to communicate with each other, with users on the Internet, and with your on-premises client computers**. You can think of an Azure network as a set of resources that links other Azure resources. Azure Virtual Networks provide the following key networking capabilities :

A diagram of a network

Description automatically generated

* Isolation and segmentation,
* Internet communications,
* communicate between Azure resources,
* communicate with on-premises resources,
* route network traffic,
* filter network traffic, and
* connect virtual networks.

1. **Isolation and segmentation,**

Virtual Network allows you to create multiple isolated virtual networks. When you set up a virtual network, you define a private IP Address space *by using either public or private IP Address ranges*. You can divide that IP Address space into sub nets on allocate part of the defined address space to each named sub net. For name resolution. You can use the name resolution service that's built into azure. You also can configure the virtual network to use either an internal or an external DNA's server.

1. **Internet communications,**

VM in Azure can connect to the Internet by default. You can enable incoming connections from the Internet by defining a public IP address or a public load balancer. For VM management, you can connect via the Azure CLI Remote desktop protocol or secure shell.

1. **Communicate between Azure resources,**

You'll want to enable azure resources to communicate securely with each other. You could do that in one of two ways.

* Virtual networks. Virtual networks can connect not only VMS but other Azure resources such as the APP service environment for power ups, Azure Kubernetes Service(AKS) on Azure virtual machine scale sets.
* Service endpoints. You can use service endpoints to connect to other azure resource types, such as as your SQLl databases and storage accounts. This approach enables you to link multiple azure resources to virtual networks to improve security and provide optimal writing between resources.

Azure virtual networks enable you to link resources together in your on premises environment and within your azure subscription. In effect, you can create a network that spans both your local and cloud environments. There are three mechanisms for you to achieve this can activity :

* **Point to site Virtual Private Networks (VPN),** The point to cite virtual private networks approach is like a virtual private network connection that a computer outside your organization makes back into your corporate network, except that it's working in the opposite direction. In this case, the client computer initiates an encrypted VPN connection to azure to connect that computer to the Azure Virtual network.
* **Site-to-site VPN**, A site to site virtual private network links your on premises VPN device or gateway to the azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the Internet.
* **Azure Express Route**, Azure Express route is the best approach for environment, where you need greater bandwidth and even higher levels of security. Express Route provides dedicated private connectivity to the azure that doesn't travel over the Internet. You'll learn more about express right later.

As your virtual networks enable you to filter traffic between sub net by using the following approaches. :

* **Network security groups**, A network security group is an azure resource that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic based on factors such a source and destination IP. Address, Port and protocol
* **Network Virtual Appliances**, a network virtual appliance is a specialized VM that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing a wide area network or one optimization.

You can link virtual networks together by using **Virtual Network Peering**. Peering enables resources in each virtual network to communicate with each other. Thes virtual networks could be in separate regions, which allows you to create a global, interconnected network through azure. **UDR is user defined routing**. UDR is a significant update to the Azure virtual networks, as this allows network admins to control the routing tables between Subnets within a sub net as well as between Venus, thereby allowing for greater control over network traffic flow.

A diagram of a computer network

Description automatically generated A diagram of a computer network

Description automatically generated

Explore Network Configuration for Virtual Machines.

**Azure Virtual Networks (AVN or VNets)** are an infrastructure as a service (IaaS) resource that allows many types of Azure resources, such a Azure VM to securely communicate with each other. They also enable some platform as a service (PaaS) resources to communicate with the internet or with on-premises networks. AVN or VNets also allow for segmentation and isolation when implementing multiple Virtual networks in Azure. In fact, Virtual networks that use VPN gateways and express row connections can act as an extension of your own data center into the cloud.

AVJ or VNets have similar capabilites than the networks you already leverage and manage on-premises. Just like your own networks, they allow you to filter and route networking traffic between hosts or subnets, allowing you to interconnect virtual networks in the same region or even across regions using network peering.

A black and white diagram of computer software

Description automatically generated with medium confidence

For added security, AVN or VNets enable you to set up defined end points to secure the traffic of your critical Azure service resources only to your virtual networks. This way, traffic always remains on the Microsoft Azure backbone. And these service endpoints can be created for the following platform as a service (PAAS) services.

* Azure Storage
* Azure SQL Database
* Azure Cosmos DB
* Azure SQL Data Warehouse
* Azure Database for MySQL
* Azure Database for PostgreSQL.

With the use of security groups and web application firewalls, AVN or VNets provide protection of your web applications and the VM hosting them from common exploits and attacks such as SQL injection and cross site scripting. In addition AVN or VNets enable you to use private IP addresses ,making it easy to integrate connections to your own data center through Express Route or site-to-site VPN gateways. This enables communication and management from the same tools and processes you already have in place for your own data centers, because it becomes just like another site in your network. And of course, you can also assign public IP addreses to Azure resources to communicate with the internet.

A computer screen with different colored icons

Description automatically generated with medium confidence

**AZURE Virtual network (AVN or VNet Setting)**

You can create and configure Azure Virtual Network (AVN) instances from the Azure portal, Azure PowerShell on your local computer, or Azure Cloud Shell.

When you create an Azure Virtual Network(AVN or VNets) , you can figure a number of basic settings. You'll have the option to configure advanced settings, such as multiple subnets, Distributed Denial of Service or DDoS Protection, and Service Endpoints. You'll configure the following settings for a basic virtual network:

* **Network name.**The network name must be unique in your subscription, but it doesn't need to be globally unique. Make the name a descriptive one that's easy to remember and identified from other virtual networks.
* **Address space**. When you set up a virtual network, you define the internal address space in classes, intra-domain routing, or CIDR format. An address space in Azure is similar to an on-premises IP addressing scheme. This address space will be unique within your subscription, *just as a subnet is within your on-premises environment*. You can then assign these address spaces to your virtual networks, ensuring there is no overlap or conflicts.
* **Subscription**; SUBSCRIPTION only applies if you have multiple subscriptions to choose from. Like any other Azure resource,a virtual network needs to exist in :
  + **a resource group**. You can either select an existing resource group, or create a new one.
  + **Location**, You will have an opportunity to select the location where you want the virtual network to exist. Within each virtual network address range, you can create one or more subnets that partition the virtual networks address space.
  + **Subnet,** Routing between subnets will then depend on the default traffic routes. You also can define custom routes. Alternatively, you can define one subnet that encompasses all that a virtual networks address ranges. Please note that subnet names must begin with a letter or number and end with a letter, number, or underscore. They may contain only letters, numbers, underscores, periods, or hyphens.

There are two types of services available:

* **Basic or Standard DDoS Protection**. Standard DDoS Protection is a premium service. For more information on Standard DDoS Protection, see Azure DDoS Protection Standard Overview on the Azure product documentation.
* **Service endpoints,** You can also enable service endpoints. You can select from a list of Azure service endpoints which ones you want to enable. Options include: Azure Cosmos DB, Azure Service Bus, Azure Key Vault, and so on.

After you've completed the configuration of these settings, you are ready to create your Azure Virtual Network. Now you can define additional settings. After you create a virtual network, you can then define further settings. These include:

* **Network security groups**, have security rules that enable you to filter the type of network traffic that can flow in and out of virtual network subnets, and network interfaces. You create the network security group separately. Then you associate it with the virtual network.
* **Route table,** Azure automatically creates a route table for each subnet within an Azure Virtual Network and add system default routes to the table. You can add custom route tables to modify traffic between virtual networks. You can also amend the service endpoints. After you've created a virtual network, you can change any further settings on the virtual network pane in the Azure portal. Alternatively, you can use PowerShell commands or commands in Cloud Shell to make changes.  You can then review and change settings and further sub-panes. You can add additional :
  + **Address spaces** to the initial definition.
  + **Connected devices,** Under connected devices, use the virtual network to connect machines.
  + **Subnets,** You can also add additional subnets, and
  + **Peerings,** under peerings you can link virtual networks in peering arrangements.
  + You can also monitor and troubleshoot virtual networks, or
  + you can create an automation script to generate the current virtual network.

Virtual networks are powerful and highly configurable mechanisms for connecting entities in Azure. You can connect Azure resources to one another or to resources you have on-premises. You can isolate, filter, and route your network traffic. Azure allows you to increase security where you feel you need it.

**Azure VPN gateway fundamentals**

**A virtual private network, or VPN, is a type of private, interconnected network. VPNs use an encrypted tunnel within another network**. They're typically deployed to connect two or more trusted private networks to one another over an untrusted network typically, the public internet. Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks. For our tailwind, trade of scenario VPNs can enable branch offices to share sensitive information between locations.

A map of the world with blue circles

Description automatically generated

For example, let's say that your office is on the East Coast region of North America need to access your company's private customer data. Which is stored on servers that are physically located in a West Coast region. A VPN that connects your East Coast offices to your West Coast servers allows your company to securely access your private customer data.

**A VPN gateway is a type of virtual network gateway**. Azure VPN gateway instances are deployed in azure virtual network instances on enable the following connectivity:

* **Site to site**, Connect on premises data centers to virtual networks through a site to site connection.
* **Point-to-site,** Connect individual devices to virtual networks through a point to site connection.
* **Network-to-network,** Connect virtual networks to other virtual networks through a network to network connection.

All transfer data is encrypted in a private tunnel as it crosses the internet. You can deploy only one VPN gateway in each virtual network, but you can use one gateway to connect to multiple locations, which includes other virtual networks or on premises data centers. When you deploy a VPN gateway, you specify the VPN type, either (**The main difference between these two types of VPNs is how traffic to be encrypted is specified**.In azure both types of VPN gateways use a pre shared key as the only method of authentication.):

* **Policy based**

Policy-based VPNs gateways specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel where that packet is going to be sent through. Key features of policy based VPN gateways in azure include :

* **Support for IKEV1 only.** *IKE or internet key exchange is a protocol used to set up a secure, authenticated communications channel between two parties*.
* **Use of static routing**, where combinations of address prefixes from both networks control high traffic, is encrypted and decrypted through the VPN tunnel. The source and destination of the tunnel networks are declared in the policy and don't need to be declared in routing tables.
* **Use policy-based VPNs where required,** Policy-based VPN must be used in specific scenarios that require them, such as for compatibility with legacy on premises VPN devices
* **Route based**.

You can use route based gateways if defining which IP addresses are behind each tunnel is too cumbersome. with route-based gateways IP SEC tunnels are modeled as a network interface or virtual tunnel interface. IP routing either static rights or dynamic routing protocols, decides which one of these tunnel interfaces to use when sending each packet. Right-based VPNs are the preferred connection method for on premises devices**. They're more resilient to topology changes such as the creation of new sub nets**. Use a right-based VPN gateway if you need any of the following types of connectivity.

* + **Connections between virtual networks**,
  + Point-to-site connections.
  + Multisite connections,
  + Co existence with an azure express route gateway.

Key features of route-based VPN gateways in azure include :

* **IKEv2 support**,
* **Wildcard traffic selectors,** use of any to any wild card traffic selectors
* **Dynamic routing protocols,** use of dynamic writing protocols for writing, forwarding tables direct traffic to different IP SEC tunnels.

In this case, the source and destination networks aren't statically defined as they are in policy-based VPNs, or even in right based VPNs with static routing. Instead, data packets are encrypted based on network writing tables that are created dynamically using routing protocols such as Border Gateway Protocol or BGP.

The capabilities of your VPN gateway are determined by the skew or size that you deploy. This table shows the main capabilities of each available skew/size.

A white background with black text

Description automatically generated

Note that a basic VPN gateway should only be used for Dev test workloads. In addition, **it's unsupported** to migrate from basic to the VPN Gw 1/2/3 Az skews at a later time without having to remove the gateway and redeploy.

Before you can deploy a VPN gateway, you'll need some azure and on premises resources. You'll need one of these azure resources before you can deploy an operational VPN gateway.

* **Virtual Network**, Deploy a virtual network with enough address space for the additional subnet that you'll need for the VPN gateway. The address space for this virtual network must not overlap with the on premises network that you'll be connecting to. You can deploy only one VPN gateway within a virtual network.
* **Gateway subnet,** Deploy a subnet called Gateway SubNet for the VPN gateway. *Use at least a forward /27 address* mask to make sure you have enough IP addresses in the subnet for future growth, you can't use this subnet for any other services.
* **Public IP address,** Create a basic skew dynamic public IP address If you're using a non zone aware gateway, This address provides a public rideable IP address as the target for your on premises VPN device. This IP address is dynamic, but it won't change unless you delete and recreate the VPN gateway.
* **Local Network gateway,** Create a local network gateway to define the on premises networks configuration, such as where the VPN gateway will connect and what it will connect to. The configuration includes the on premises VPN devices public IPv4 address on the on premises rideable networks. This information is used by the VPN gateway to write packets that are destined for on premises networks through the IP SEC tunnel.
* **Virtual network Gateway,** Create the virtual network gateway to write traffic between the virtual network on the on premises data center or other virtual networks. The virtual network gateway could be either a VPN or express route gateway, but this unit only deals with VPN virtual network gateways. You'll learn more about express route in a separate unit later in this module.
* **Conntction,** Create a connection resource to create a logical connection between the VPN gateway on the local network gateway. The connection is made to the on the premises VPN devices IPV4 address as defined by the local network gateway. The connection is made from the virtual network gateway on its associated public IP address.

This diagram shows the combination of resources on their relationships to help you better understand what's required to deploy a VPN gateway.

A screenshot of a computer

Description automatically generated

To connect your data center to a VPN gateway there are some required on premises resources:

* **A VPN device**, a VPN device that supports policy-based or route based VPN gateways.
* **A public facing IPv4 address**, A public-facing internet writable IP address.

A diagram of a computer process

Description automatically generated

There are several ways to ensure you have a fault tolerant configuration. By default, VPN gateways are deployed as two instances in an active stand by configuration. Even if you only see one VPN gateway resource in Azure. When planned maintenance or unplanned disruption affects the active instance. The standby instance automatically assumes responsibility for connections without any user intervention. Connections are interrupted during this fail over but they're typically restored within a few seconds for planned maintenance on within 90 seconds for unplanned disruptions.

With the introduction off support for the BGP writing protocol, you could also deploy VPN gateways in an active-active configuration. In this configuration, you assign a unique public IP address to each instance. You then create separate tunnels from the on premises device to each IP address. You can extend the high availability by deploying an additional VPN device on premises.

Another high availability option is to configure a VPN gateway as a secure, fail over path for express route connections. Express route circuits have resiliency built in, but they aren't immune to physical problems that affect the cables delivering connectivity or outages that affect the complete express route location. In high availability scenarios where there's risk associated with an outage open express route circuit, you could also provision of VPN gateway that uses the internet as an alternative method of connectivity. In this way, you can ensure there's always a connection to the virtual networks.

In regions that support availability zones, VPN, gateways and express right gateways could be deployed in **a zone-redundant configuration.** This configuration brings a resiliency, scalability and higher availability to virtual network gateways. Deploying gateways in azure availability zones physically and logically separates gateways within a region while protecting your on premises network connectivity to azure from zone level failures. These gateways require different gateway, skews/size and use standard public IP addresses instead of basic public IP addresses.

**Azure ExpressRoute fundamentals**

ExpressRoute lets you exchange your on premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute you can establish connections to Microsoft Cloud services such as Microsoft Azure on Microsoft 365.

Connectivity can be from any to any pipe VPN network, a point to point ethernet network or a virtual cross connection through a connectivity provider at a co location facility.

A diagram of a computer connection

Description automatically generated ExpressRoute connections don't go over the public Internet, this allows express route connections to offer more reliability, faster speeds, consistent latencies on higher security than typical connections over the Internet. For information on how to connect your networks to Microsoft using ExpressRoute see express route connectivity models.

As part of your work for tailwind traders, you should understand what as your ExpressRoute is and how it integrates with on premises and as your networks.

Now we will cover the benefits that ExpressRoute provides compared to other site to site connectivity options. As a result, you'll learn whether express route could provide your company with the best possible network performance throughout. This unit will focus on two different layers of the open systems interconnection or OSI model.

* **Layer 2** or L2 is the dazzling glare, which provides note to note communication between two nodes on the same network.
* **Layer 3** or L3 is the network layer, which provides addressing and writing between nodes on a multi node network.

There are several benefits to using ExpressRoute as the connection service between azure and on premises networks :

* **Layer 3 connectivity** between your on premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from any to any IP VPN network, a point to point ethernet connection or through a virtual cross connection via an ethernet exchange.
* **Connectivity to Microsoft cloud** services across all regions in the geopolitical region.
* **Global connectivity to Microsoft services** across all regions with the ExpressRoute premium add on.
* **Dynamic routing** between your network on Microsoft via Border Gateway Protocol (BGP)
* **Built in redundancy** in every peering location for higher reliability
* **Connection up time SLA** and
* **QOS support for Skype for business**.

ExpressRoute provides :

* **Layer 3 connectivity,** layer three address level connectivity between your on premises network on the Microsoft Cloud through connectivity partners. These connections could be from a point to point or any to any network, they can also be virtual cross connections through an exchange.
* **Built in redundancy,** Each connectivity provider uses redundant devices to ensure that connection's established with Microsoft are highly available. You can configure multiple circuits to complement this feature. All redundant connections are configured with a layer three connectivity to meet service level agreements (SLA).
* **Connectivity to Microsoft Cloud services**, ExpressRoute enables connectivity to Microsoft Cloud Services that includes direct access to the following services in all regions.
  + Microsoft Office 365,
  + Microsoft Dynamics 365,
  + Azure compute services such as Azure virtual machines,
  + Azure cloud services such as Azure Cosmos DB and Azure Storage. Office 365 was created to be accessed securely and reliably via the Internet. For this reason, we recommend the use of ExpressRoute for specific scenarios.

You can enable express route global reach to exchange data across your on premises sites by connecting your ExpressRoute circuits. For example, assume that you have a private data center in California connected to ExpressRoute in Silicon Valley. You have another private data center in Texas, connected to ExpressRoute in Dallas. With ExpressRoute global reach, you can connect your private data centers through to ExpressRoute circuits. Your cross data center traffic will travel through the Microsoft Network **.ExpressRoute uses the Border Gateway Protocol or BGP routing protocol**. BGP is used to exchange routes between on premises networks on resources running in azure. This protocol enables dynamic routing between your on premises network and services running in the Microsoft Cloud.

A diagram of different types of internet connection

Description automatically generated

ExpressRoute supports three models that you can use to connect your on premises network to the Microsoft Cloud.

1. Cloud Exchange Co-location

**Colocation at a cloud exchange**, Co-located providers can normally offer both Layer 2 and Layer 3 connections between your infrastructure, which might be located in the co location facility on the Microsoft Cloud. For example, If your data center is co-located at a cloud exchange such as an ISP, you can request a virtual cross connection to the Microsoft Cloud.

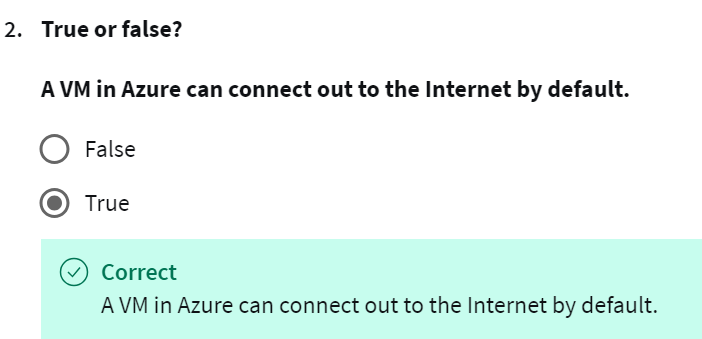
1. Point to point Ethernet connection

Point-to-point connections provide layer 2 and layer 3 connectivity between your on premises site and azure. You can connect your offices or data centers to azure by using the point to point links. For example, if you have an on premises data center, you can use a point to point ethernet link to connect to Microsoft.

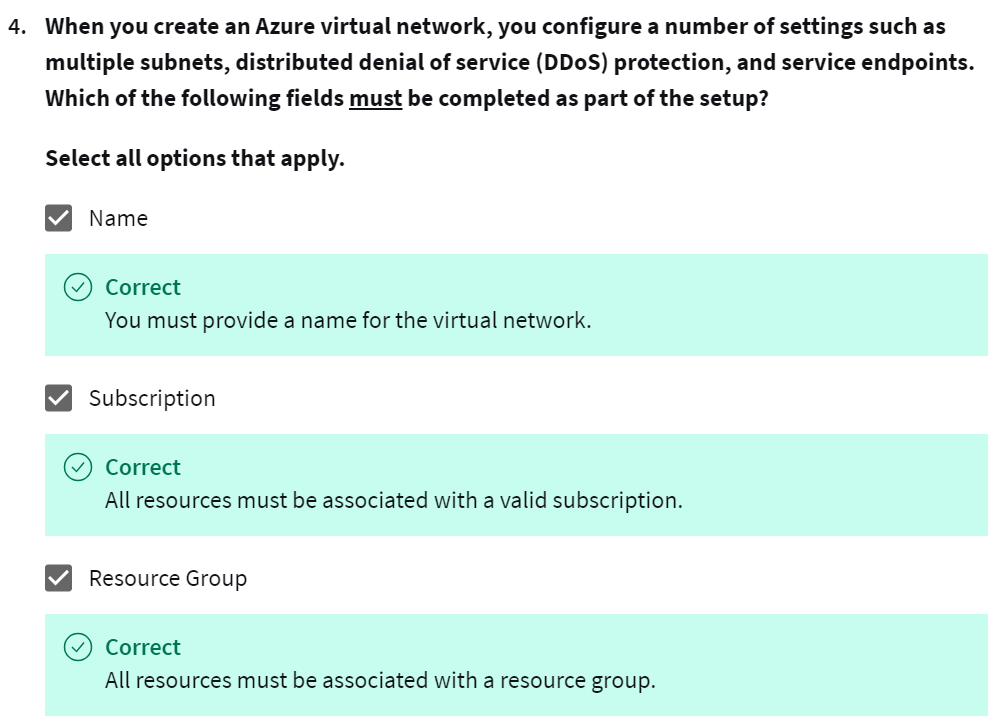
1. Any to any connection.

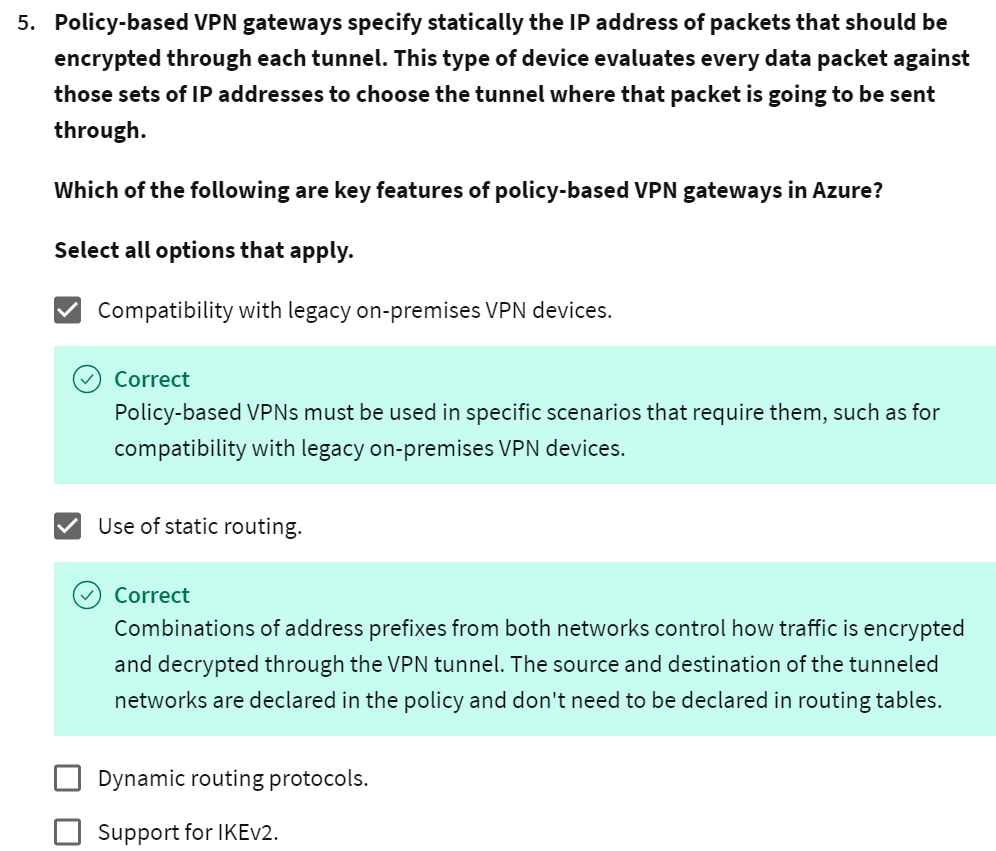
With any-to-any connectivity, you can integrate your wide area network with azure by providing connections to your offices and data centers. Azure integrates with your WAN connection to provide a connection like you would have between your data center and any branch offices. With any-to-any connections, all WAN providers offer layer three connectivity. For example, if you already use multi protocol label switching to connect to your branch offices or other sites in your organization on ExpressRoute connection to Microsoft behaves like any other location on your private WAN. With ExpressRoute, your data doesn't travel over the public Internet, so it's not exposed to the potential risks associated with Internet communications. **ExpressRoute is a private connection from your own premises infrastructure to your Azure infrastructure, even if you have an ExpressRoute connection** DNA's Queries , Certificate Revocation list Checking on as your content delivery network requests are still sent over the public Internet.

A screenshot of a computer

Description automatically generated 

A screenshot of a computer

Description automatically generated 

 A screenshot of a computer

Description automatically generated

* 1. You use service endpoints to connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach enables you to link multiple Azure resources to virtual networks, thereby improving security and providing optimal routing between resources.
  2. A VM in Azure can connect out to the Internet by default.
  3. That’s correct. A network security group is an Azure resource that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol.
  4. A network virtual appliance is a specialized VM that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing Wide Area Network (WAN) optimization.
  5. When you create an Azure virtual network, you configure a number of settings such as multiple subnets, distributed denial of service (DDoS) protection, and service endpoints. Which of the following fields must be completed as part of the setup? **Name, Subscription and Resource Group**
  6. Policy-based VPN gateways specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel where that packet is going to be sent through.

Which of the following are key features of policy-based VPN gateways in Azure?

* Use of static routing.

Combinations of address prefixes from both networks control how traffic is encrypted and decrypted through the VPN tunnel. The source and destination of the tunneled networks are declared in the policy and don't need to be declared in routing tables.

* Compatibility with legacy on-premises VPN devices.

Policy-based VPNs must be used in specific scenarios that require them, such as for compatibility with legacy on-premises VPN devices.

* 1. Dynamic routing protocols, where routing/forwarding tables direct traffic to different IPsec tunnels, is a feature of Route-Based VPNs.
  2. Policy-based VPN gateways support IKEv1 only. Route-based VPNs support IKEv2
  3. Which of the following are supported ExpressRoute models that you can use to connect your on-premises network to the Microsoft cloud?
     + **Cloud Exchange colocation**, Co-located providers can normally offer both Layer 2 and Layer 3 connections between your infrastructure, which might be located in the colocation facility, and the Microsoft cloud.
     + **Any-to-any connection**, With any-to-any connectivity you can integrate your wide area network (WAN) with Microsoft Azure by providing connections to your offices and datacenters.

A close-up of a white background

Description automatically generated A screenshot of a computer

Description automatically generated

A close-up of a computer screen

Description automatically generated A screenshot of a computer

Description automatically generated

A close-up of a message

Description automatically generated A screenshot of a computer

Description automatically generated

1. Archive storage stores data offline and offers the lowest storage costs but also the highest data rehydrate and access costs.
2. Hot storage tier is optimized for storing data that is accessed frequently, like images for your website.
3. Network security groups have security rules that enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces. You create the network security group separately, and then associate it with the virtual network.
4. You connect on-premises data centers to Azure virtual networks through a site-to-site connection.
5. Azure ExpressRoute lets you seamlessly extend your on-premises networks into the Microsoft cloud. This connection between your organization and Azure is dedicated and private. Establishing an ExpressRoute connection enables you to connect to Microsoft cloud services like Azure, Office 365, and Dynamics 365. Security is enhanced, connections are more reliable, latency is minimal and throughput is greatly increased.
6. You must deploy an Azure virtual network with enough address space for the additional subnet that you’ll need for the VPN gateway. The address space for this virtual network must not overlap with the on-premises network that you’ll be connecting to.
7. You must create a Basic-SKU dynamic public IP address if using a non-zone-aware gateway. This address provides an public-routable IP address as the target for your on-premises VPN device.
8. You must create the virtual network gateway to route traffic between the virtual network and the on-premises data center or other virtual networks.

**What to expect**

The next course will cover **Azure Management Tools & Security Solutions.**

**Module 1 - AI Services & Solutions**

 In module 1, you will learn about Artificial Intelligence, or AI, Services & Solutions. You will study how to determine the Azure AI services that best address your company's business challenges and the software development process tools and services that best address specific business scenarios.

**Module 2 - Monitoring & Managing in Azure**

Module 2 will deal with Monitoring & Managing in Azure. You will learn how to choose the cloud monitoring service that best addresses your company's business challenges and the management tools that best address your organization's technical needs and challenges.

**Module 3 - Azure Serverless Technology & IoT**

In module 3, we will address Azure Serverless Technology and Internet of Things, or IoT.  You will be able to identify the serverless computing technology that best addresses your business scenario and choose the Azure IoT service that best addresses your business scenario.

**Module 4 - General Security & Network Security in Azure**

Finally, module 4, will cover General Security and Network Security in Azure. In module 4, you will learn how to:

* Strengthen your security posture and protect against threats by using Azure Security Center.
* Collect and act on security data from many different sources by using Azure Sentinel.
* Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
* Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.
* Identify the layers that make up a defense in depth strategy.
* Explain how Azure Firewall enables you to control what traffic is allowed on the network.
* Configure network security groups to filter network traffic to and from Azure resources within a Microsoft Azure virtual network.
* Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.