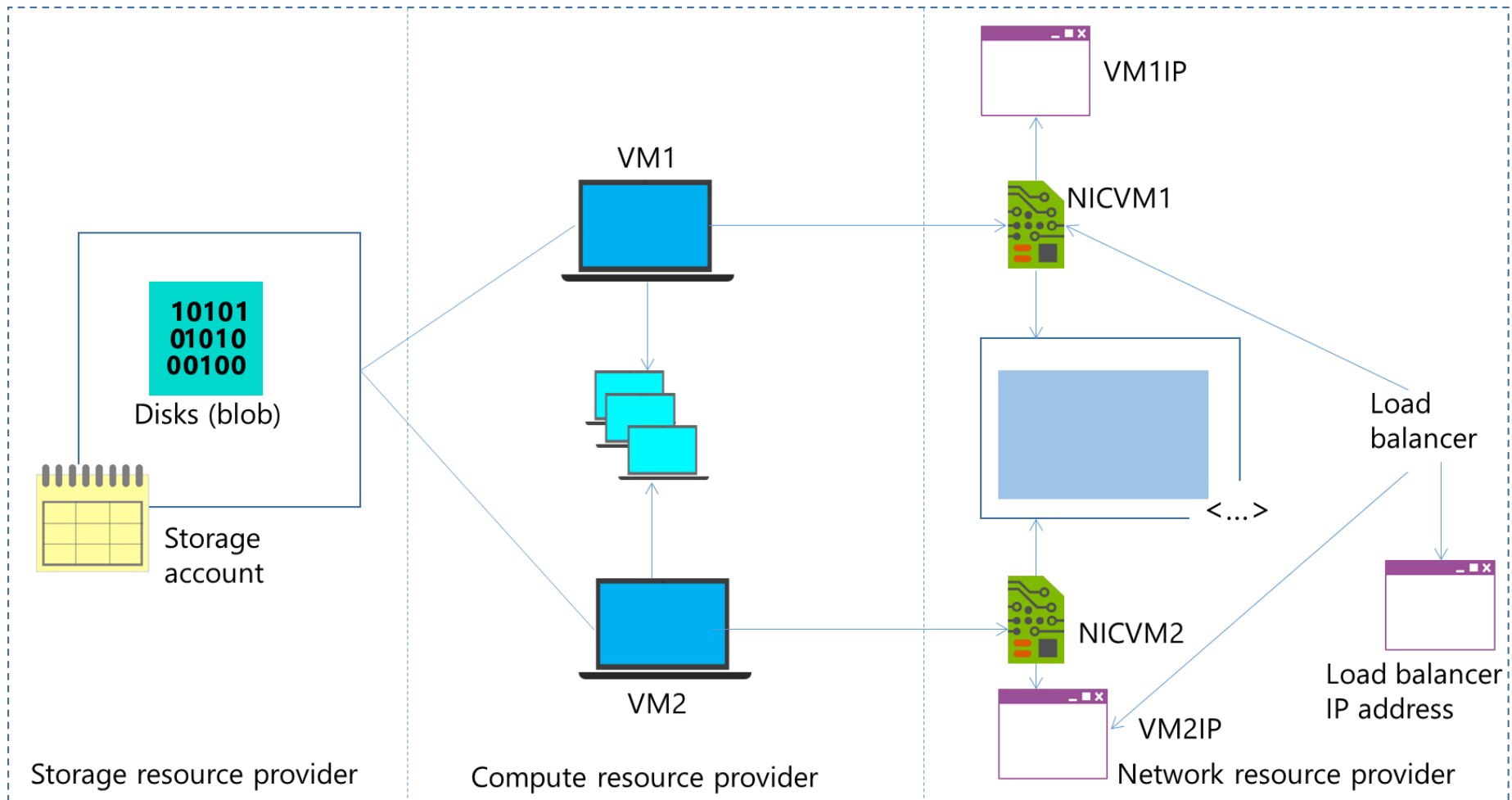# Module 2

Implementing and managing Azure networking

Module Overview

- Overview of Azure networking
- Implementing and managing virtual networks
- Configuring Azure virtual network
- Configuring virtual network connectivity
- Overview of Azure classic networking

Cloud Compute Solution

Lesson 1: Overview of Azure networking

- Demonstration: Preparing the Azure environment for the demos and labs in this module
- Azure networking components
- Overview of Azure virtual networks
- Overview of network interfaces
- Overview of private IP addresses
- Overview of load balancers
- Overview of Azure DNS

Demonstration: Preparing the Azure environment for the demos and labs in this module

In this demonstration, you will learn how to:

- Sign in to your Azure subscription
- Prepare the Azure environment

Note: To prepare the lab environment for this module, you must complete the above tasks

Azure networking components

Compute

- Service Fabric
- Container Service
- Azure Virtual Machines
- Azure Cloud Services

Networking

- Virtual Network
- Azure DNS
- Application Gateway
- Traffic Manager
- ExpressRoute
- Load Balancer

Data & Storage

- Storage
- DocumentDB
- Azure SQL Database
- StorSimple

Web & Mobile

- Web Apps
- Mobile Apps
- Notification Hub

Other services

- Service Bus
- Azure AD
- Azure AD DS
- MFA
- Automation
- Scheduler
- Azure Backup
- Site Recovery
- Key Vault
- Azure Security Center

Azure networking components

- VNets
- IP Addresses:
    - Private IP addresses
    - Public IP addresses
- Subnets
- Network interfaces
- DNS
- Azure load balancer and internal load balancer
- Application gateway

- Traffic Manager
- Network Security Groups
- User-defined routes
- Forced Tunneling
- Regional VNets
- Cross-premises network connectivity
    - A Point-to-Site VPN
    - A Site-to-Site VPN
    - ExpressRoute

VNet features:

- Azure Resource Manager deployment model:
  - Private IP addresses, allocated to a NIC
  - Public IP addresses, allocated to a NIC or a load balancer
- Azure Classic deployment model:
  - Dynamic IP addresses, allocated to a VM
  - Virtual IP addresses, allocated to a cloud service
  - Public instance-level IP addresses, allocated to a VM
- IP addressing in VNets
- Subnets
- DNS
- VNet connectivity

Overview of network interfaces

- NIC:
  - Assign to a VM
  - Assign to a load balancer backend pool
- IP address configuration:
  - Private IP addresses with dynamic and static allocation
  - Public IP addresses with dynamic and static allocation
- Multiple NIC configuration for VMs:
  - VM based on size D1_v2 – single NIC
  - VM based on size D2 _v2 – two NICs
  - VM based on size D3_ v2 – four NICs
  - VM based on size D4_v2 – eight NICs

Overview of private IP addresses

- Private IP address allocation:
  - Dynamic
  - Static
- Adding a static private IP address:
  1. *$vnet* = **Get-AzureRmVirtualNetwork –ResourceGroupName AdatumRG -Name AdatumVNet**
  2. *$subnet* = **$vnet.Subnets[0].Id**
  3. *$nic* = **New-AzureRmNetworkInterface -Name AdatumNIC -ResourceGroupName AdatumRG -Location centralus -SubnetId $vnet.Subnets[0].Id –PrivateIpAddress 192.168.0.10**
  4. **Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id**

Overview of load balancers

- Azure load balancer:
  - Internal load balancer
  - Internet-facing load balancer
- Application gateway
- Traffic Manager
- Configuring Azure load balancer:
  - Configure front-end IP
  - Configure backend address pool
  - Create load-balancing rules
  - Create health probes
  - Create inbound NAT rules

Overview of Azure DNS

Creating an Azure DNS zone and a DNS record:

1. Select the subscription:

   Select-AzureRmSubscription –SubscriptionName <Name of your subscription>

2. Create a new resource group:

   New-AzureRMResourceGroup –Name AdatumRG –Location centralus

3. Create a DNS Zone:

   New-AzureRmDnsZone -Name adatum.com -ResourceGroupName AdatumRG

4. Retrieve SOA and NS records for the zone:

   Get-AzureRmDnsRecordSet -ZoneName adatum.com –ResourceGroupName AdatumRG

5. Create a resource record:

   New-AzureRmDnsRecordSet -Name "www" -RecordType "A" -ZoneName "adatum.com" -ResourceGroupName "AdatumRG" -Ttl 60

Overview of Azure DNS

Record type	Full name	Function
A (IPv4) AAAA (IPv6)	Address	Maps a host name such as www.adatum.com to an IP address, such as 131.107.10.10
CNAME	Canonical name	Points one host record, such as ftp.adatum.com, to another host record, such as host1.adatumcom
MX	Mail exchange	Points to the host that will receive mail for that domain. MX records must point to an A record, and not to a CNAME record
NS	Name server	Contains the name of a server hosting a copy of the DNS zone
SOA	Start of Authority	Provides information about the writable copy of the DNS zone, including its location and version number
SRV	Service	Points to hosts that are providing specific services, such as the Session Initiation Protocol (SIP) endpoint or Active Directory domain controllers
TXT	Text	Records a human-readable text field in DNS

Lesson 2: Implementing and managing virtual networks

- Planning for Azure virtual networks
- Using the Azure portal to create virtual networks
- Using PowerShell to create virtual networks
- Using an Azure Resource Manager template to create a virtual network
- Demonstration: Deploying a virtual network by using an Azure Resource Manager template

Planning for Azure virtual networks

- Choose either private or public non-overlapping address space
- Create subnets:
  - The first three IP addresses and the last IP address within each subnet are not available for use
  - The smallest subnets you can specify use 29-bit subnet masks
- Use static, private IP addresses (optional)

Using the Azure portal to create virtual networks

1. Sign in to the Azure Portal
2. In the navigation menu on the left, click **New,** select **Networking**, and then click **Virtual Network**
3. On the **Virtual Network** blade, verify that Resource Manager deployment model is selected, and then click **Create**
4. On the **Create virtual network** blade, in the **Name** text box, type a descriptive name for the Vnet
5. In the **Address space** box, select an IP address range by using CIDR notation
6. In the **Subnet name** text box, type a descriptive name for the subnet
7. In the **Subnet address range** box, type the IP address range for the subnet using CIDR notation
8. In the **Subscription** box, select the right Azure subscription in which you want to create a virtual network
9. In the **Resource group** box, either create a new resource group or select an existing one
10. In the **Location** box, select a location near your users, and click **Create**

Using PowerShell to create virtual networks

1. Start Microsoft Azure PowerShell session and sign in to your subscription
2. Select the subscription in which you plan to create a virtual network
3. Create a new resource group
4. Create a new VNet and address space
5. Add a subnet to the virtual network
6. Update the configuration of the virtual network

Using an Azure Resource Manager template to create a virtual network

Demonstration: Deploying a virtual network by using an Azure Resource Manager template

In this demonstration, you will see how to implement a VNet by using an Azure Resource Manager template

Lab A: Using a deployment template and Azure PowerShell to implement Azure virtual networks

- Exercise 1: Creating an Azure virtual network by using a deployment template
- Exercise 2: Creating a virtual network by using PowerShell
- Exercise 3: Configuring virtual networks

Estimated Time: 30 minutes

A. Datum Corporation's Azure VMs currently reside on a classic virtual network in the branch region. To prepare for deployment of Azure Resource Manager VMs, A. Datum must deploy an Azure Resource Manager virtual network in the Headquarters region. You determined this is a relatively straightforward process if you use an existing deployment template and modify its parameters during deployment. However, you want to also test deployment of a virtual network by using Azure PowerShell.

In addition, you need to prepare your existing classic virtual network for establishing connectivity to the Azure Resource Manager virtual network by creating a virtual network gateway and deploy a test Azure Resource Manager VM to the virtual network deployed by using the template.

What are the methods that you can use to create an Azure classic virtual network?

Lesson 3: Configuring Azure virtual network

- Configuring name resolution in Azure virtual network
- Configuring User Defined Routes
- Configuring forced tunneling
- Configuring network security groups
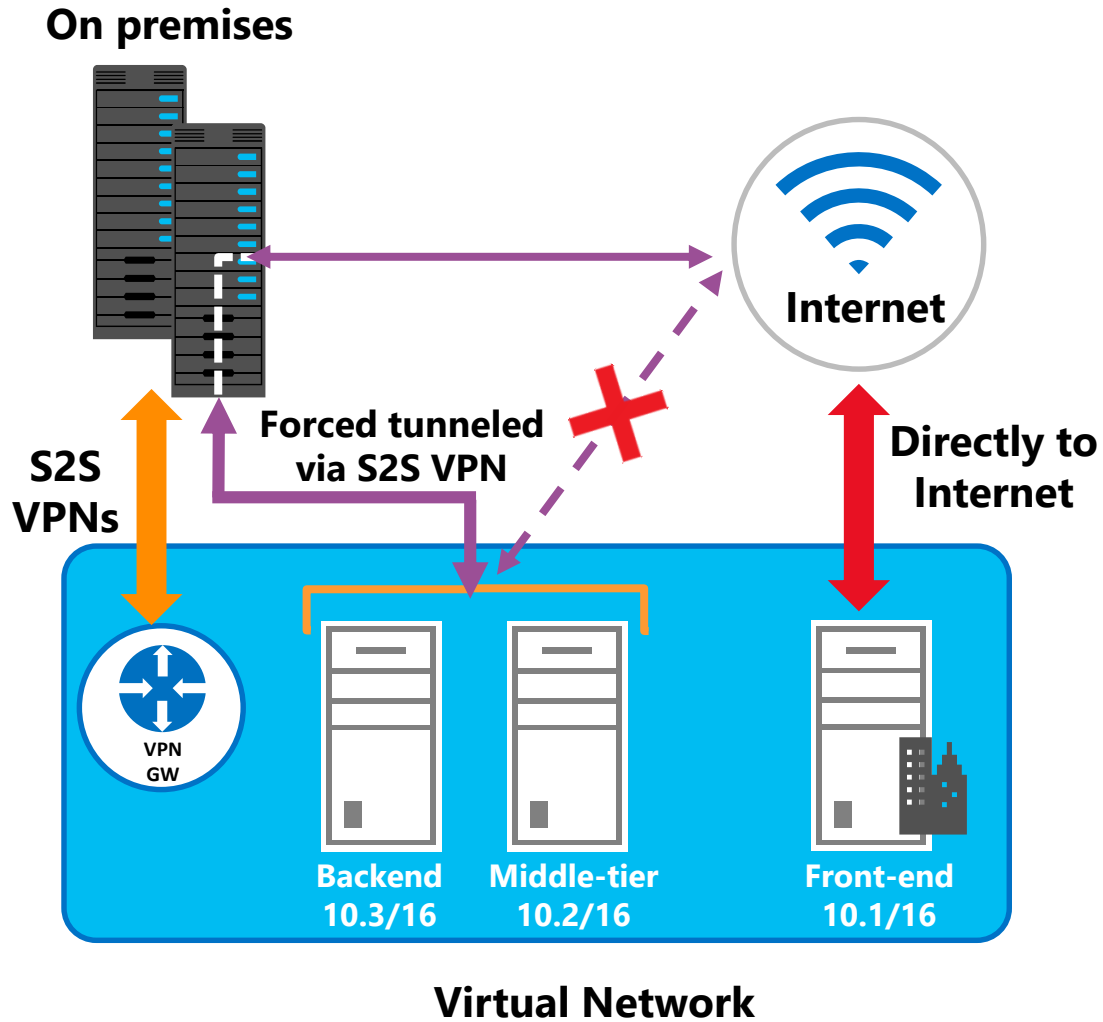- Demonstration: Configuring network security groups

Configuring name resolution in Azure virtual network

Scenario	Location	Name resolution provision
Between classic VMs	Same cloud service	Use Azure-provided name resolution
Between Azure Resource Manager VMs	Same VNet	Use Azure provided name resolution or a custom DNS
Between role instances or classic VMs	Same VNet but different cloud services	Use a custom DNS. With FQDN-based name resolution, you can use Azure name resolution for the first 100 cloud services
Between VMs or role instances and on-premises computers	Azure VNets and on-premises	Use a custom DNS server
Between VMs	Different VNets	Use a custom DNS server
Reverse lookups of internal IP addresses	Azure Vnet	Use a custom DNS server

Configuring User Defined Routes

- System routes contain the following rules:
  - Local VNet rule
  - On-premises rule
  - Internet rule
- User defined routes contain the following information:
  - Address prefix
  - Next hop type:
    - Local
    - VPN gateway
    - Internet
    - Virtual appliance
    - NULL
  - Next hop value

Configuring forced tunneling

Configuring network security groups

Network security group rules consist of:

- Name
- Direction
- Priority
- Access
- Source IP address prefix
- Source port range
- Destination IP address prefix
- Destination port range
- Protocol

Demonstration: Configuring network security groups

In this demonstration, you will see how to create a network security group and associate it with a subnet of a virtual network

Lesson 4: Configuring virtual network connectivity

- Azure virtual network connectivity options
- Configuring point-to-site VPN connectivity
- Configuring a site-to-site VPN
- Configuring a VNet-to-VNet VPN
- Connecting classic and Azure Resource Manager-based virtual networks in different Azure regions

Azure virtual network connectivity options

Azure

West US VNet

East US VNet

VNet-to-VNet

ExpressRoute

Point-to-site

Site-to-site

On-premises network
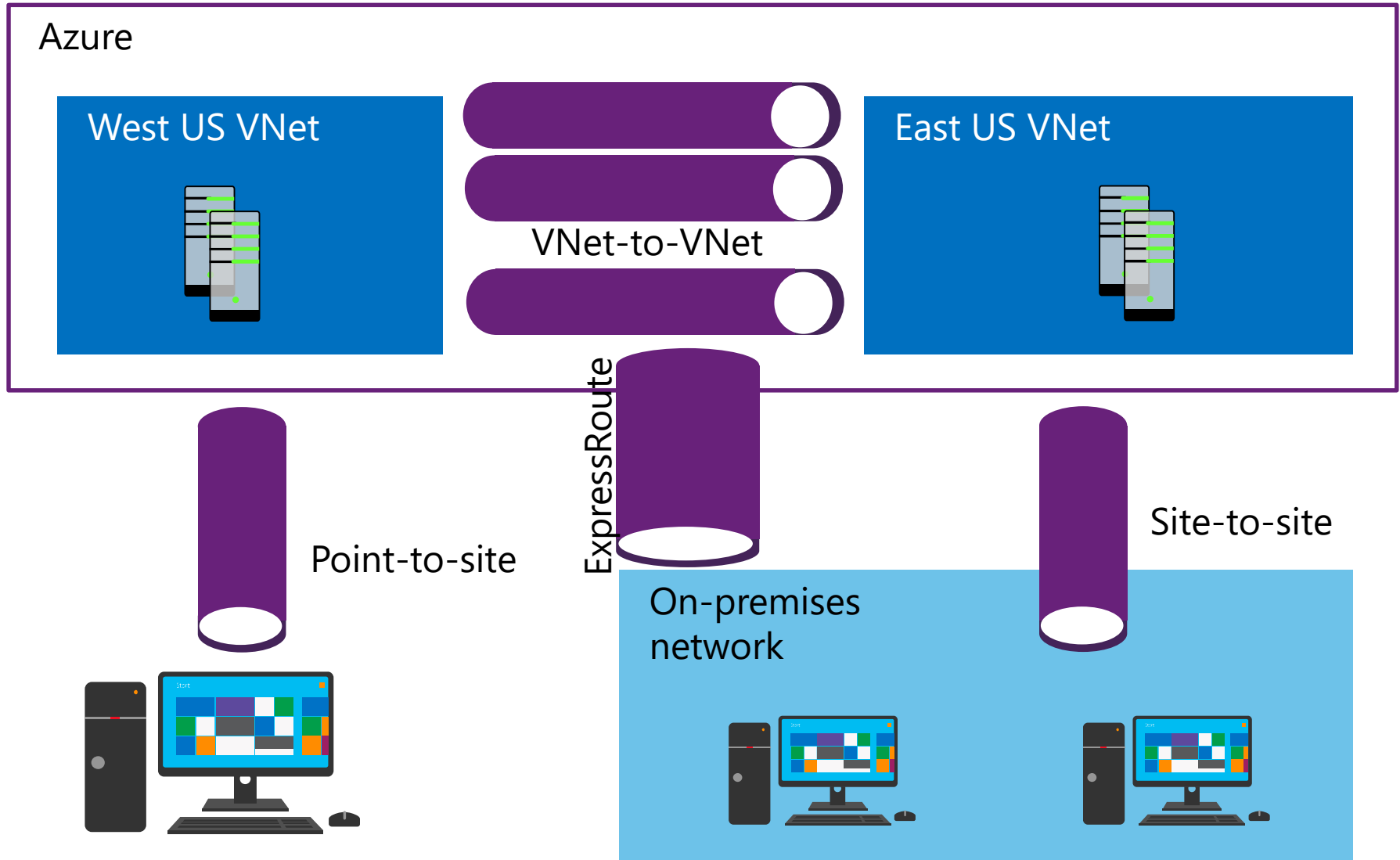
Configuring point-to-site VPN connectivity

1. Configure an IP address space for clients
2. Configure a virtual gateway
3. Create root and client certificates
4. Create and install the VPN client configuration package
5. Connect via the VPN

Configuring a site-to-site VPN

1. Connect to your Azure subscription
2. Create a new custom VNet and gateway subnet
3. Add a local site
4. Request a public IP address for the VPN device
5. Create a virtual gateway
6. Configure a VPN device
7. Create a VPN connection
8. Verify the VPN connection

Configuring a VNet-to-VNet VPN

1. Connect to your Azure subscription
2. Create the first virtual network
3. Request a public IP address, and create the gateway configuration
4. Create the gateway
5. Create the second virtual network and its gateway
6. Connect the VPN gateways

1. Create an ARM VNet
2. Create a classic VNet
3. Connect the classic and the ARM VNets

- Overview of classic virtual networks
- Connecting to classic virtual networks
- Implementing a classic virtual network

Overview of classic virtual networks

- Cloud services and virtual machines
- IP addresses:
  - DIP addresses
  - VIP addresses
  - Static IP addresses
  - Reserved IP addresses
  - Instance-level PIP addresses
- DNS
- Azure load balancer and internal load balancer

Connecting to classic virtual networks

To connect to classic virtual networks, use:

- Point-to-site

- Site-to-site

- VNet-to-VNet

- ExpressRoute

- VNet peering (only for connectivity to Azure Resource Manager Vnets)

Implementing a classic virtual network

1. From the **NETWORKS** page in the Azure classic portal, open the VNet Custom Create Wizard

2. Set the VNet name and select a region

3. Configure a DNS server if required

4. Configure IP address name spaces and subnets according to your plan

Implementing a virtual network in classic

Configuring a VNet by using a configuration file:

```xml
<VirtualNetworkSites>
  <VirtualNetworkSite name="Main_Network" Location="East
      Asia">
    <AddressSpace>
      <AddressPrefix>192.168.0.0/16</AddressPrefix>
    </AddressSpace>
    <Subnets>
      <Subnet name="Front-End Subnet">
        <AddressPrefix>192.168.0.0/28</AddressPrefix>
      </Subnet>
      <Subnet name="Mid-Tier Subnet">
        <AddressPrefix>192.168.0.16/29</AddressPrefix>
      </Subnet>
      <Subnet name="Back-End Subnet">
        <AddressPrefix>192.168.0.24/29</AddressPrefix>
      </Subnet>
    </Subnets>
  </VirtualNetworkSite>
</VirtualNetworkSites>
```

Lab B: Configuring connectivity between classic and Azure Resource Manager virtual networks

- Exercise 1: Using a PowerShell script to connect a classic VNet and an Azure Resource Manager VNet

- Exercise 2: Configuring a point-to-site VPN

- Exercise 3: Validating virtual network connectivity

Estimated Time: 35 minutes

Now that A. Datum has deployed an Azure Resource Manager VNet, the company wants to be able to provide direct connectivity to the classic VMs on the existing classic VNet. To allow for direct communication between VMs on both virtual networks, you need to implement VNet-to-VNet connection between them. You will accomplish this by modifying and running an Azure PowerShell script. You also want to implement a point-to-site VPN, so that you can connect from your administrative computer.

Lab Review

- What are the key steps for configuring a point-to-site VPN?

- How can you enable communications between VMs that are created with the Azure classic deployment model and VMs that are created with the ARM model?

Module Review and Takeaways

- Best Practices
- Common Issues and Troubleshooting Tips
- Review Question