Module 2

Implementing and managing Azure networking

Module Overview

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

Lesson 1: Overview of Azure networking

- Demonstration: Preparing the lab environment
- 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 lab environment

In this demonstration, you will learn how to prepare the lab environment

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

Azure networking components

Compute
- **Virtual Machines**
- **Virtual Machine Scale Sets**
- **Cloud Services**
- Containers
- Container Registry
- **Container Service**

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

Data & Storage
- Disk Storage
- Blob Storage
- File Storage
- Queue Storage
- Table Storage
- StorSimple

Web & Mobile
- Web Apps
- Mobile Apps
- Logic Apps
- Content Delivery Network

Other services
- Azure AD
- **Azure AD DS**
- Azure B2C
- MFA
- Automation
- Backup
- **Site Recovery**
- Log Analytics
- Azure Monitor
- Azure Advisor
- Key Vault
- Network Watcher
- Azure Security Center

Azure networking components

- Virtual networks and subnets
- Network interfaces
- IP addresses (private and public)
- Virtual network-based DNS and Azure DNS
- Azure Load Balancer
- Application Gateway
- Traffic Manager
- Network security groups
- Service endpoints
- User-defined routes
- Forced tunneling
- Virtual network connectivity
- Virtual network gateways

Overview of Azure virtual networks

- An IP address space with one or more subnets:
  - Private:
    - 10.x.x.x
    - 172.16.x.x – 172.31.x.x
    - 192.168.x.x
  - Public (supported, but rarely used)
- IP addresses
  - Private - allocated to VM NICs or internal load balancers
  - Public - assigned to VM NICs or load balancers
- DNS name resolution
  - Default – Internet names and names within the virtual network
  - Custom – cross-premises, cross-virtual networks, custom domains (Active Directory)

Virtual network connectivity

- Cross-premises:
  - Point-to-Site
  - Site-to-Site
  - ExpressRoute
- Cross-virtual network (the same or different Azure regions:
  - VNet peering (different Azure regions in public preview)
  - VNet-to-VNet
- Virtual gateways:
  - VPN gateways
  - ExpressRoute gateways

Overview of network interfaces

- Multi-network adapter VMs:
  - Network adapters can be added during or post VM deployment
    - Azure PowerShell or Azure CLI
  - Max limit depends on the VM size (ranges from 2 to 8)
  - All VMs must be on the same virtual network
  - Primary network adapter: Default gateway
  - Secondary network adapters: By default, no routing beyond local subnet
- IP address configurations:
  - Multiple IP configurations per network adapter are supported
  - Each IP configuration consists of:
    - A mandatory private static or dynamic IP address
    - An optional public static or dynamic IP address

Overview of private IP addresses

- Private IP address allocation:
  - Dynamic
  - Static

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

    ```
    az network nic create --resource-group AdatumRG --name AdatumNIC \
      --location centralus --subnet default --private-ip-address 192.168.0.10 \
      --vnet-name AdatumVNet
    ```

Overview of load balancers

- Azure Load Balancer (layer 4):
  - Internal or internet-facing
  - Basic SKU:
    - across 100 VM instances: a standalone VM, Azure VMs in the same availability set, or a VM scale set
    - single subnet
  - Standard SKU:
    - across 1000 VM instances: any combination of standalone VMs, Azure VMs, and VM scale sets
    - multiple subnets in the same virtual network
- Application Gateway (layer 7):
  - Internal or internet-facing
  - Azure VMs, Cloud Service instances, Azure web apps
- Traffic Manager (DNS-based):
  - Internet facing
  - Any public IP address with a DNS name

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 record set:

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

6. Create a resource record:

   Add-AzureRmDnsRecordConfig -RecordSet $AdatumRs -Ipv4Address 110.15.15.110

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	Assigns a custom name, such as ftp.adatum.com, to a host record, such as host1.adatumcom
MX	Mail exchange	Points to the host that accepts email for the 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) or Active Directory Domain Services
TXT	Text	Contains custom text

Lesson 2: Implementing and managing virtual networks

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

Planning for Azure virtual networks

- Choose one or more IP address spaces:
  - Private or public
  - Non-overlapping (recommended)
- Divide an IP address space into one or more subnets:
  - The first three IP addresses and the last IP address within each subnet are reserved by the platform
  - The smallest subnets you can specify use 29-bit subnet masks, with three usable IP addresses
- Moving VMs between subnets:
  - Supported within the same virtual network
  - Not supported across virtual networks

Using the Azure portal to create virtual networks

1. In the hub menu, click **+ Create a resource**, select **Networking**, and then click **Virtual Network**

2. On the **Create virtual network** blade, in the **Name** text box, type a name of the VNet

3. In the **Address space** box, specify an IP address space in CIDR notation

4. In the **Subscription** box, select the right Azure subscription in which you want to create a virtual network

5. In the **Resource group** box, either create a new resource group or select an existing one

6. In the **Location** box, select the Azure region where the VNet will reside

7. In the **Subnet** section, in the **Name** text box, type a name for the first VNet subnet

8. In the **Subnet** section, in the **address range** box, type the IP address range for the subnet using CIDR notation

9. Enable or disable **Service endpoints** for the subnet.

10. Click **Create**

Using Azure PowerShell to create virtual networks

1. Start 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 Azure CLI to create virtual networks

1. Start an Azure CLI 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 subnet

Using Azure PowerShell to create a virtual network based on an Azure Resource Manager template

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 Azure PowerShell

- Exercise 3: Creating a virtual network by using Azure CLI

Logon Information
Virtual machine: **20533E-MIA-CL1**
User name: **Student**
Password: **Pa55w.rd**

Estimated Time: 30 minutes

Lab Scenario

Adatum Corporation plans to create several virtual networks in their Azure subscription. They will all reside in the same Azure region. You want to test the deployment of Azure virtual networks by using both imperative and declarative methods.

Lab Review

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

Lesson 3: Configuring an Azure virtual network

- Configuring name resolution in an Azure virtual network
- Configuring user-defined routes
- Configuring forced tunneling
- Configuring network security groups
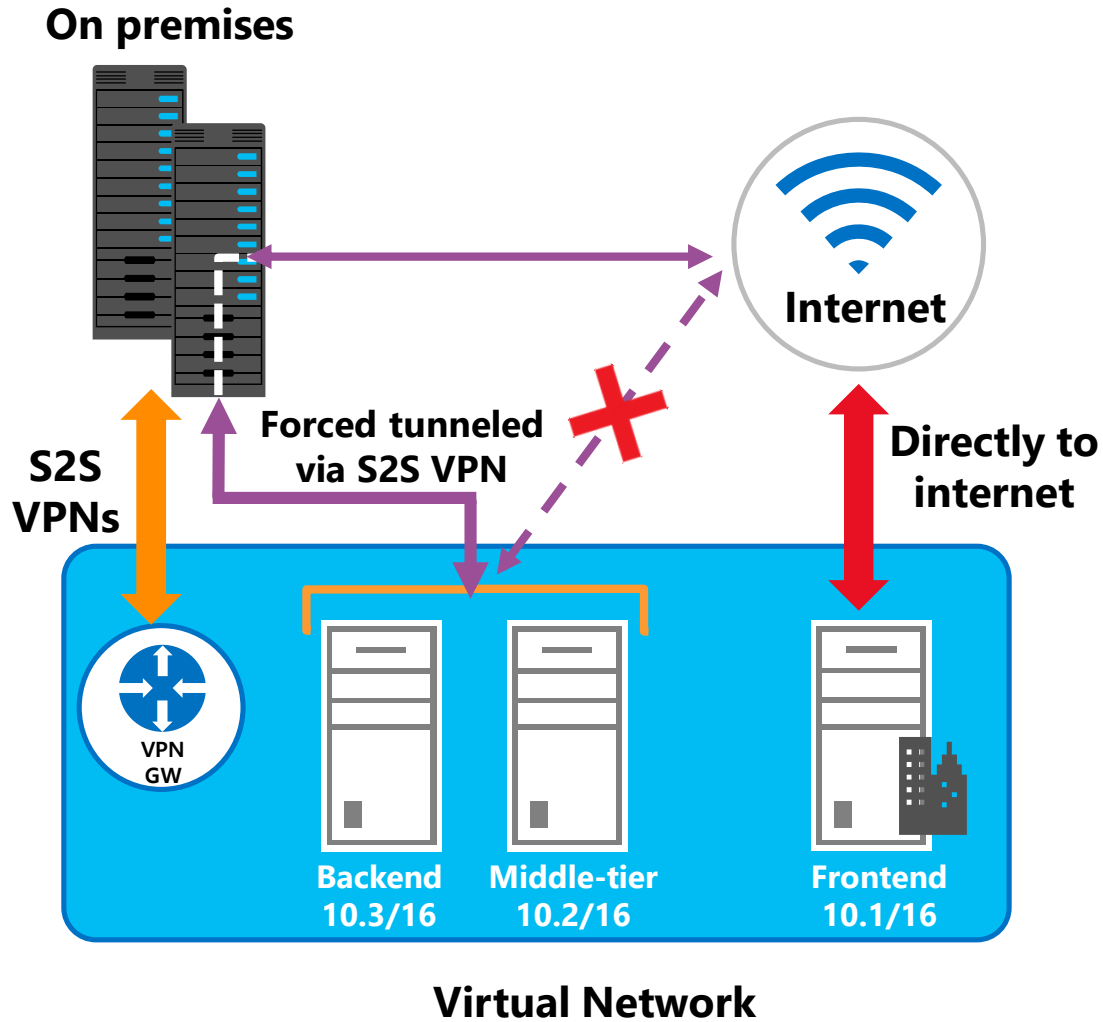- Demonstration: Configuring network security groups

Configuring name resolution in an Azure virtual network

Scenario	Location	Name resolution provision
Between Azure VMs	Same VNet	Use Azure provided name resolution or a custom DNS
Between Azure VMs 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
Private DNS domain names	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:
    - Virtual network
    - Virtual gateway
    - Internet
    - Virtual appliance
    - None
  - Next hop value

Configuring forced tunneling

Configuring network security groups

Network security group rules consist of:
- Name
- Direction
- Priority
- Source
- Source port range
- Destination
- Destination port range
- Protocol
- Action

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 P2S VPN connectivity
- Configuring a site-to-site VPN
- Configuring a VNet-to-VNet VPN
- Configuring VNet Peering

Azure virtual network connectivity options
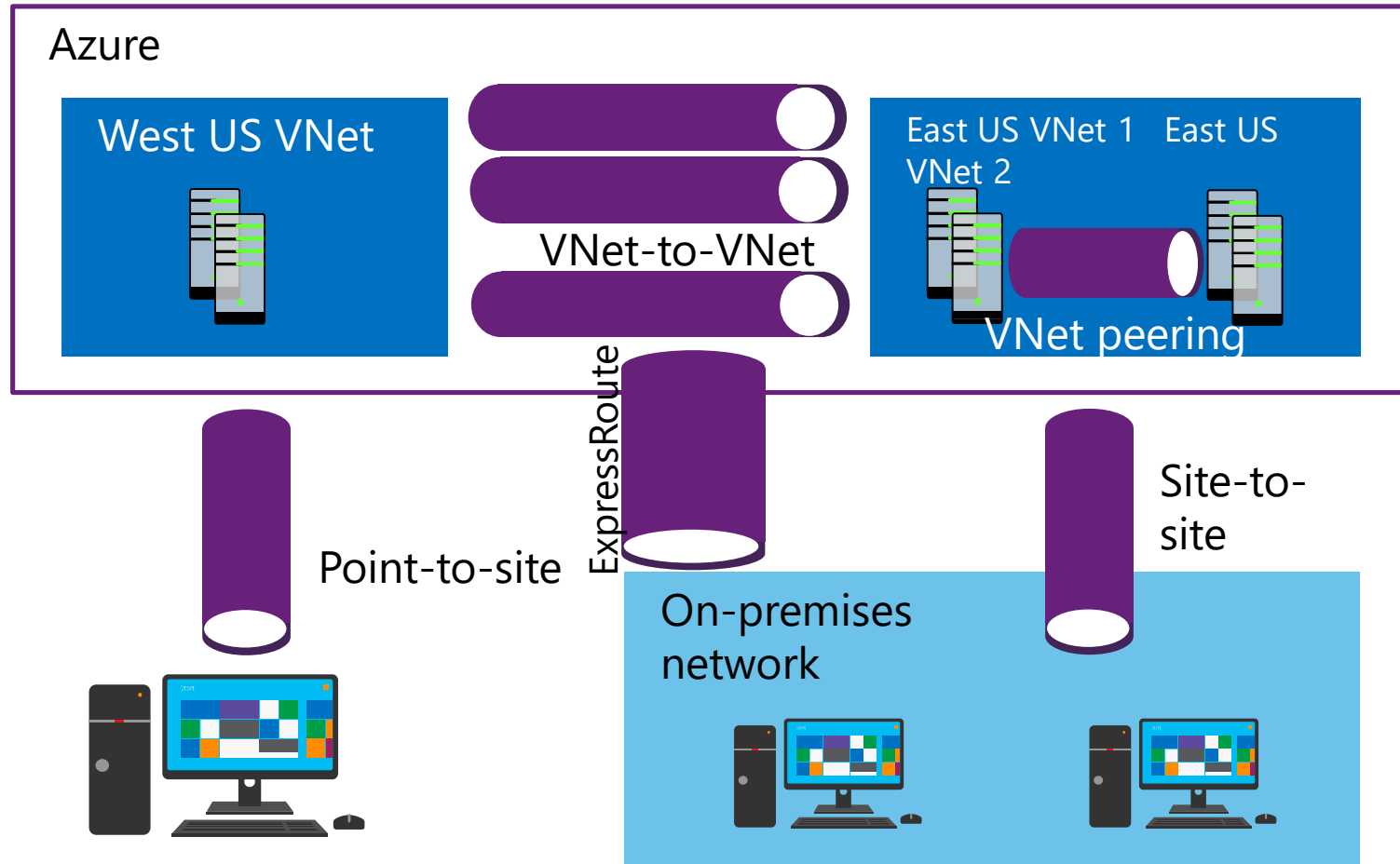
Configuring P2S VPN connectivity

Configure point-to-site VPN with certificate-based authentication

1. Create a virtual network and gateway subnet
2. Generate root and client certificates
3. Create a VPN gateway
4. Upload the root certificate to the VPN gateway
5. Distribute client certificates to VPN clients
6. Generate the VPN client configuration package
7. Install the VPN client configuration package

Configure point-to-site VPN with RADIUS-based authentication

1. Create a virtual network and gateway subnet
2. Set up the RADIUS server
3. Create a VPN gateway
4. Configure the VPN gateway as a RADIUS client
5. Generate the VPN client configuration package
6. Install the VPN client configuration package

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

Configuring VNet Peering

1. Connect to your Azure subscription
2. Create the first virtual network
3. Create the second virtual network
4. Configure VNet peering in the first virtual network
5. Configure VNet peering with the matching settings in the second virtual network
6. Verify the VNet peering status

Lab B: Configuring VNet Peering

- Exercise 1: Using the Azure portal to configure VNet Peering

- Exercise 2: Configuring VNet Peering–based service chaining

- Exercise 3: Validating virtual network connectivity

Logon Information

Virtual machine: **20533E-MIA-CL1**
User name: **Student**
Password: **Pa55w.rd**

Estimated Time: 35 minutes

Now that Adatum Corporation has deployed Azure Resource Manager VNets, the company wants to be able to provide direct connectivity between them. Your plan is to implement VNet Peering to provide the optimal performance with minimum cost.

- What do you consider to be the most important advantages of VNet Peering?

Module Review and Takeaways

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