Azure Virtual Networks

Topics

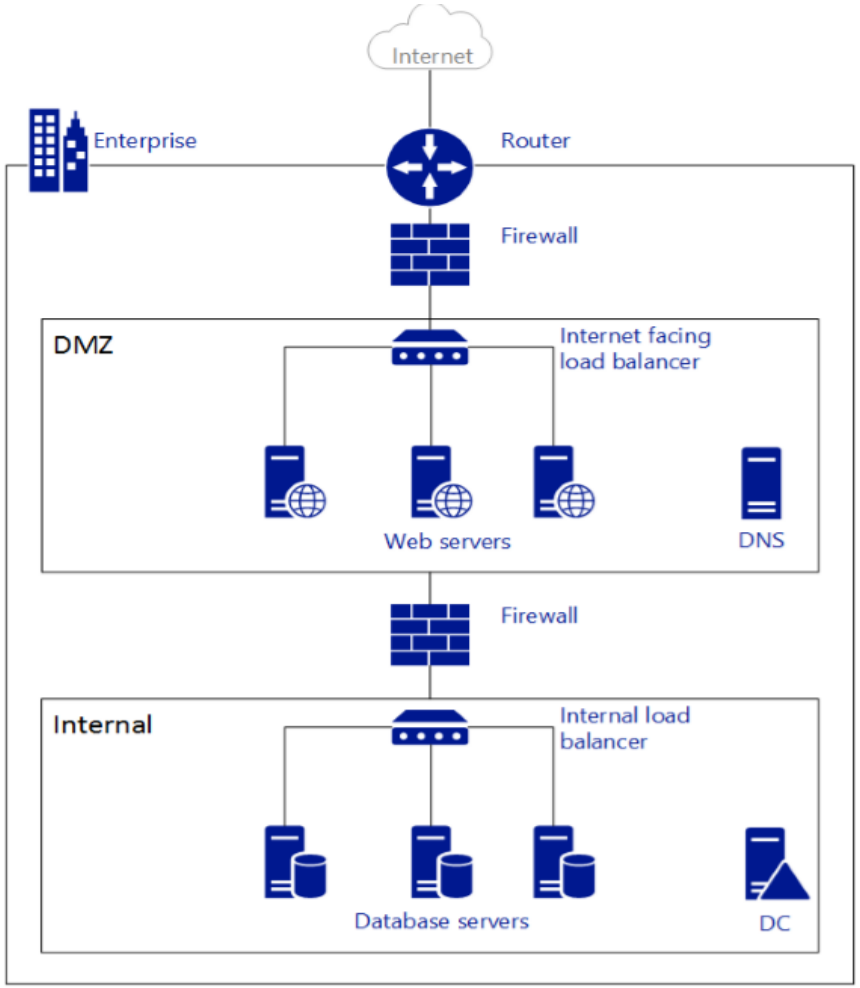
Introduction

Planning and Implementing Virtual Networks

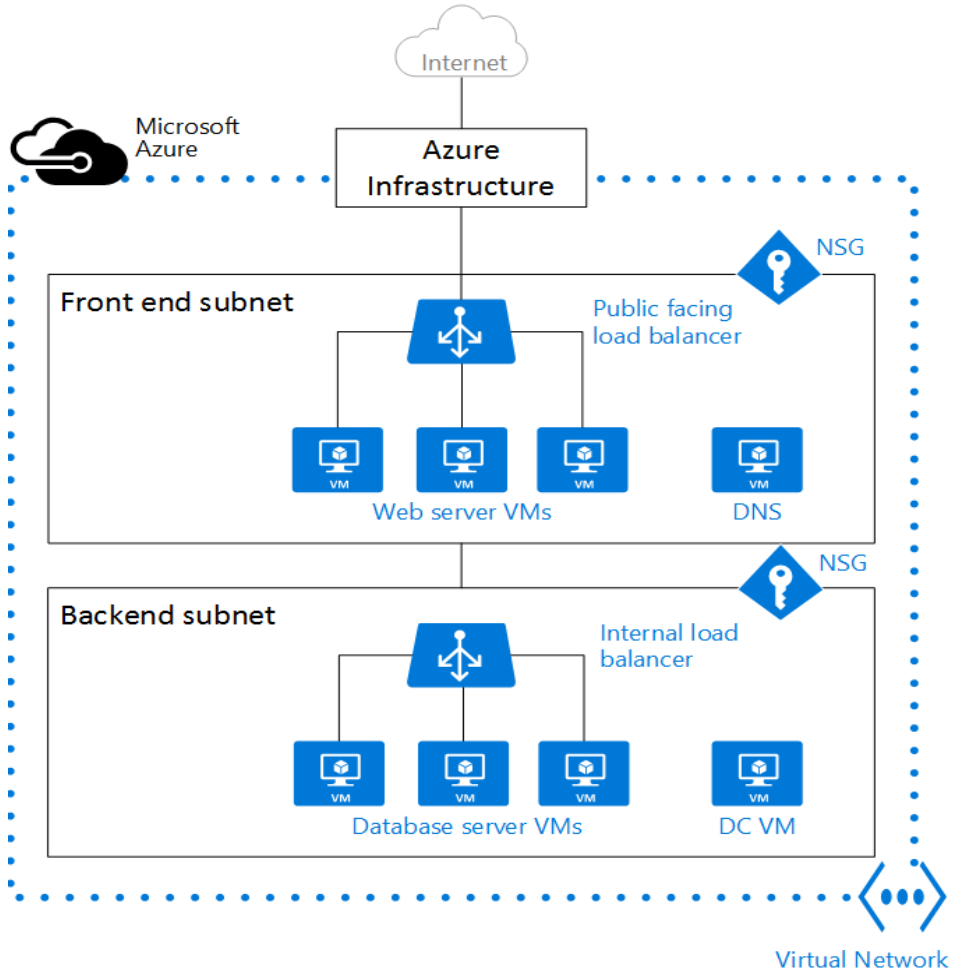
Inter-Site Connectivity

Introduction

Virtual Networks



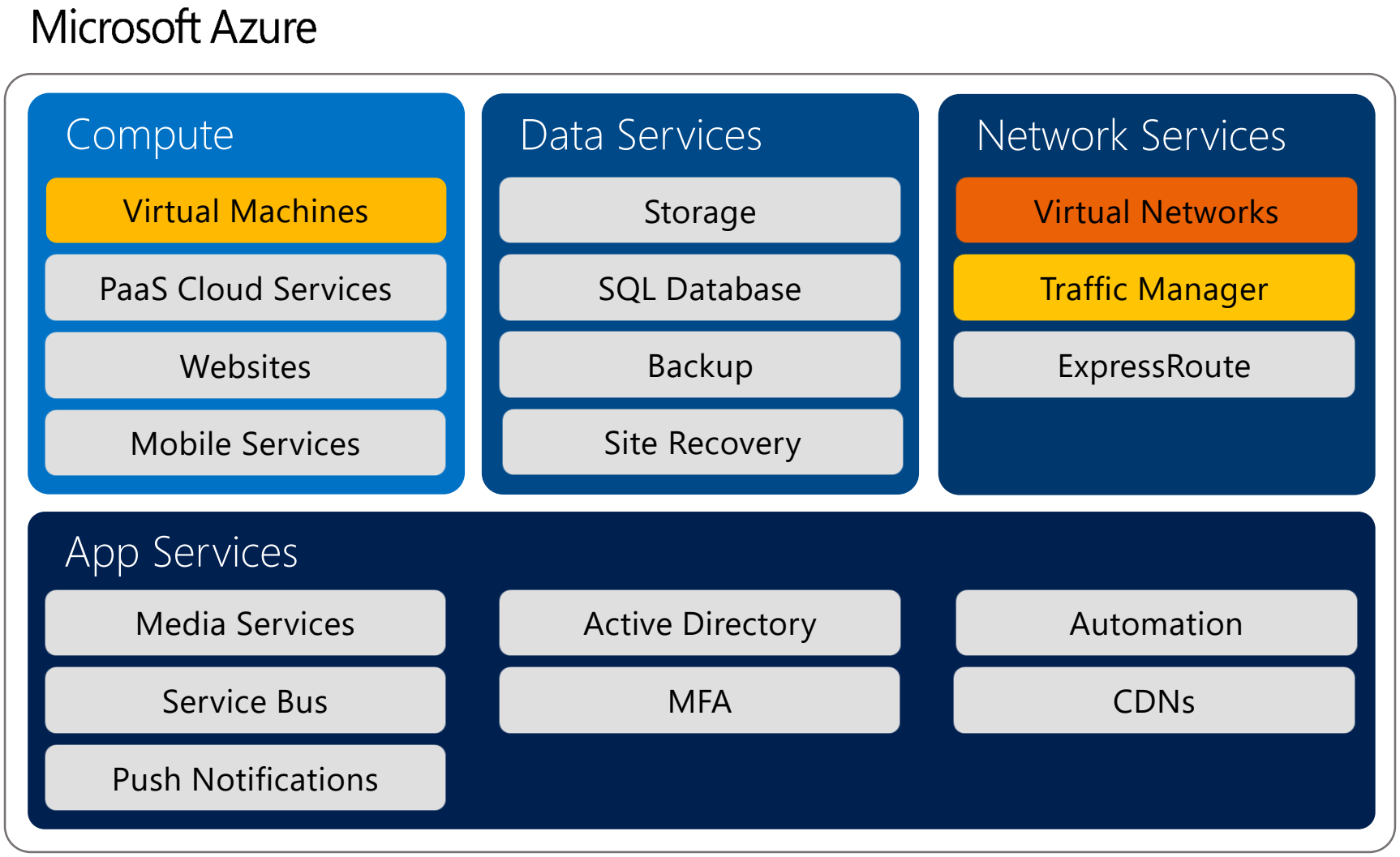
VS



On-Premise Networking

Azure Virtual Networking

Virtual Networks



Azure Networking Components

- Cloud services and virtual machines
- IP addresses
  - Virtual IP addresses
  - Dynamic IP addresses
  - Reserved IP addresses
  - Instance-level Public IP addresses
- DNS
- Azure Load Balancer and Internal Load Balancer
- Traffic Manager
- Regional VNets

Virtual Network Benefits

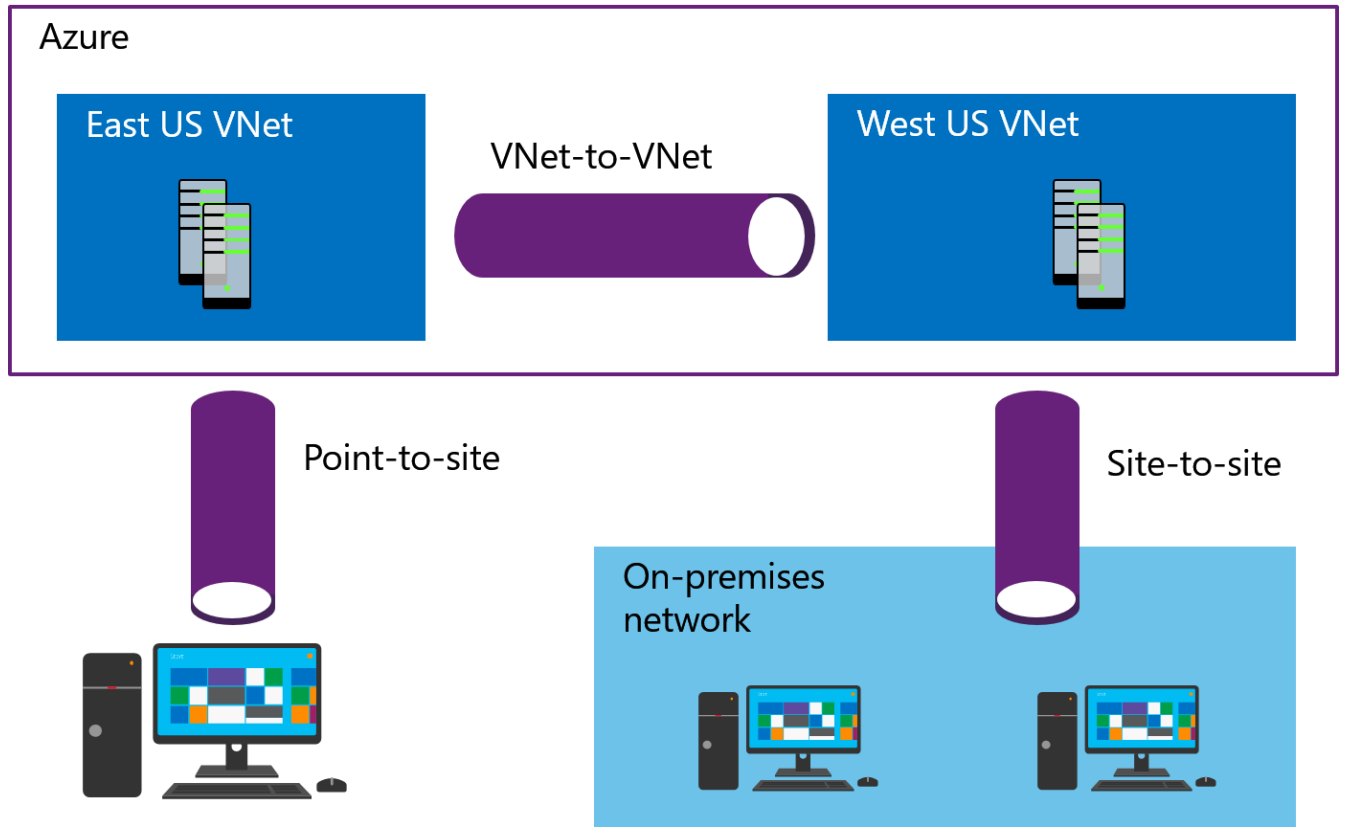
- Isolation
- Access to the public Internet
- Access to VMs within the VNet
- Name Resolution
- Security
- Connectivity

Connecting to Virtual Networks

- Cloud-only virtual networks
  - Use endpoints to connect to specific services
- Point-to-site VPNs
  - Use a VPN to connect from a single computer
- Site-to-site VPNs
  - Use a VPN to connect from an on-premise subnet
- Vnet-to-Vnet VPNs
  - Use a VPN to connect between two VNets.
- ExpressRoute
  - Connect directly without going over the Internet

Inter-Site Connectivity Options

- Point-to-Site VPN
- Site-to-Site VPN
- VNET to VNET



Planning and Implementing Virtual Networks

Designing IP Address Space and Subnet Allocation in Azure Virtual Networks

- Choose a private non-overlapping address space:
  - 10.0.0.0/16
  - 172.16.0.0/12
  - 192.168.0.0/16
- Choose 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
- Optionally use static internal IP addresses

Create Virtual Networks

- Azure Portal
  - Classic
  - New Portal
- Configuration file
- Powershell / CLI

Create VNets using new portal

1. From the Networks page, start 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.

Configuring an IaaS v1 VNet using a configuration file

```
<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>
```

Configuring an IaaS v1 VNet using a configuration file

1. Download or create NetworkConfig.XML file:

```
Get-AzureVNetConfig
  -ConfigurationPath "C:\NetworkConfig.XML"
```

2. Edit the NetworkConfig.XML file
3. Use Set-AzureVNetConfig to update the VNet configuration:

```
Set-AzureVNetConfig
  -ConfigurationPath "C:\NetworkConfig.XML"
```

Create an IaaS v2 VNet using PowerShell

- Install and configure Azure PowerShell, by following the steps in the How to Install and Configure Azure PowerShell article.
- If necessary, create a new resource group, as shown below.

```
New-AzureRmResourceGroup -Name TestRG -Location centralus
```

- Create a new Vnet

```
$vnet = New-AzureRmVirtualNetwork -ResourceGroupName TestRG -
Name TestVNet -AddressPrefix 192.168.0.0/16 -Location centralus
```

- Add a subnet to the new VNet variable and repeat

```
Add-AzureRmVirtualNetworkSubnetConfig -Name FrontEnd `
-VirtualNetwork $vnet -AddressPrefix 192.168.1.0/24
```

- save the changes to Azure

```
Set-AzureRmVirtualNetwork -VirtualNetwork $vnet
```

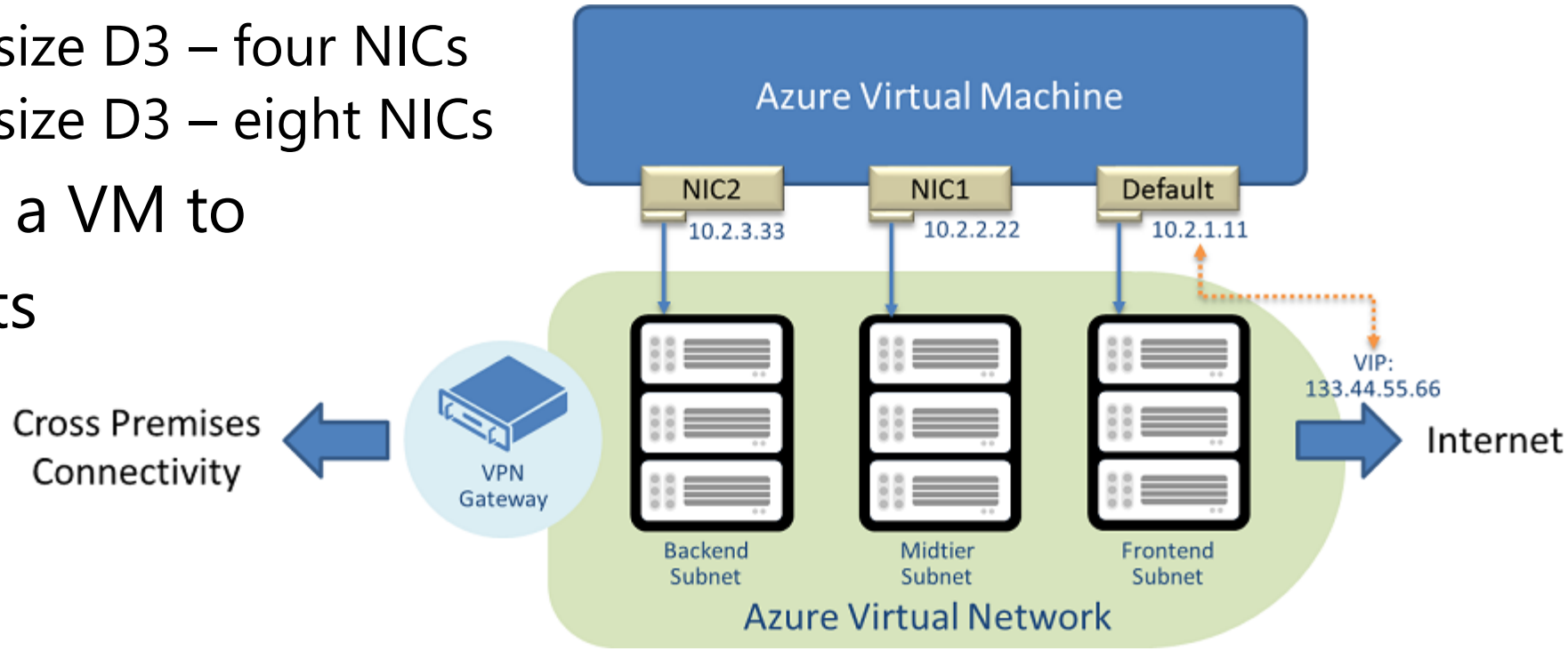
Deploying a VM into a Virtual Network

Creating a VM in a VNet:

1. Use the FROM GALLERY option.
2. Select an image.
3. Enter a VM name and set credentials.
4. Specify a IaaS cloud service name.
5. Select a VNet and Subnet.

Using Multiple NICs

- Multiple NIC configuration for VMs, or Virtual Appliance:
  - VM based on size D1 – Single NIC
  - VM based on size D2 – two NICs
  - VM based on size D3 – four NICs
  - VM based on size D3 – eight NICs
- Use to connect a VM to multiple subnets



Using Multiple NICs

- Internet-facing VIP (classic deployment) is only supported on the “default” NIC. There is only one VIP to the IP of the default NIC
- Address for each NIC on each VM must be located in a subnet
  - Multiple NICs on a single virtual machine can each be assigned addresses on the same subnet
- Work must be done in PowerShell, CLI or via ARM. Not supported in portal

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
- Create using portal or PowerShell

Configuring Network Security Groups

- PowerShell cmdlets (classic)
  - New-AzureNetworkSecurityGroup
  - Set-AzureNetworkSecurityRule

- PowerShell cmdlets (Resource Manager)
  - New-AzureRMNetworkSecurityRuleConfig
  - New-AzureRMNetworkSecurityGroup
  - Set-AzureRMVirtualNetworkSubnetConfig

Default Rules —— Inbound

Inbound default rules

Name	Priority	Source IP	Source Port	Destination IP	Destination Port	Protocol	Access
ALLOW VNET INBOUND	65000	VIRTUAL_NETWORK	*	VIRTUAL_NETWORK	*	*	ALLOW
ALLOW AZURE LOAD BALANCER INBOUND	65001	AZURE_LOADBALANCER	*	*	*	*	ALLOW
DENY ALL INBOUND	65500	*	*	*	*	*	DENY

Default Rules —— Outbound

Outbound default rules

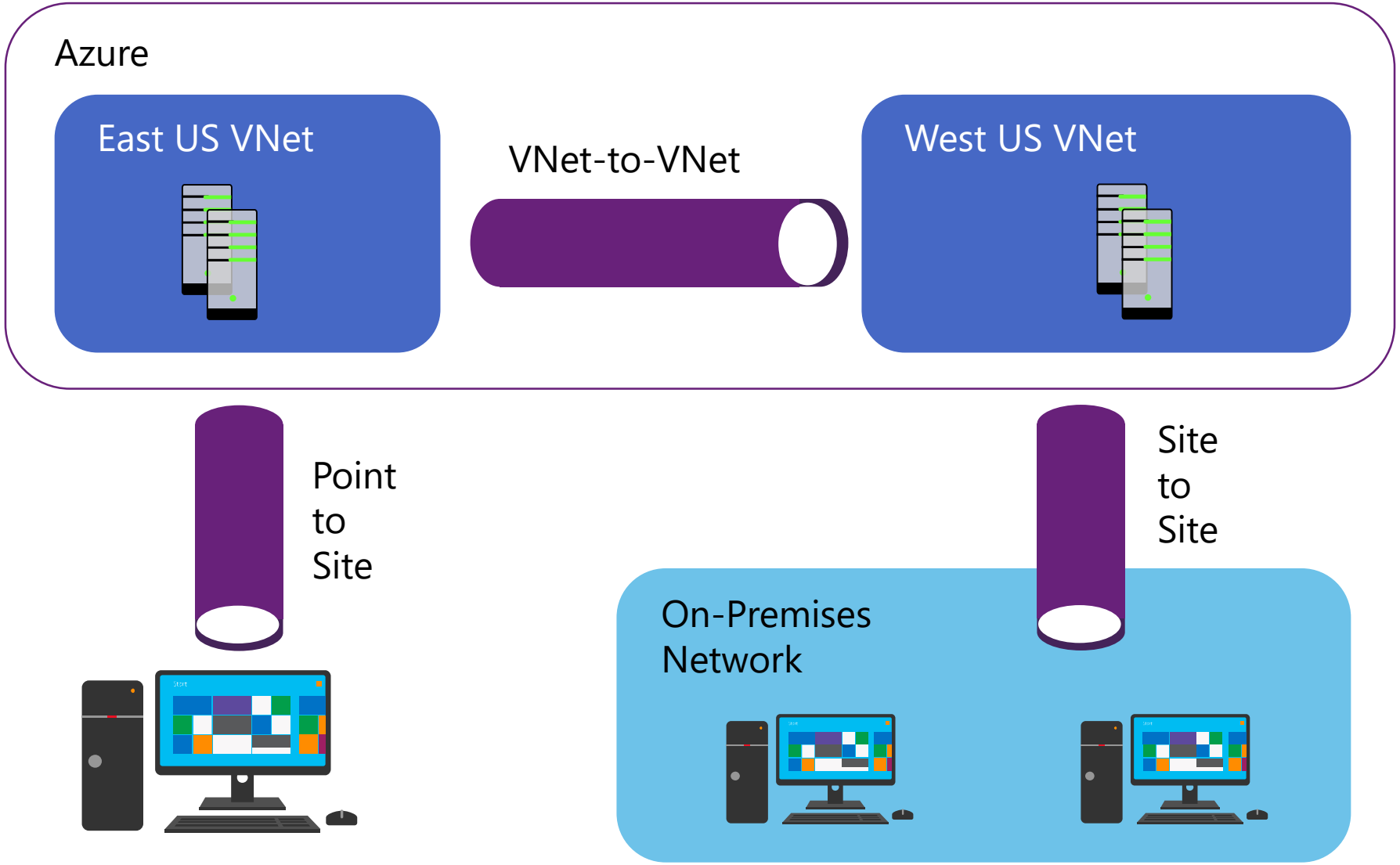
Name	Priority	Source IP	Source Port	Destination IP	Destination Port	Protocol	Access
ALLOW VNET OUTBOUND	65000	VIRTUAL_NETWORK	*	VIRTUAL_NETWORK	*	*	ALLOW
ALLOW INTERNET OUTBOUND	65001	*	*	INTERNET	*	*	ALLOW
DENY ALL OUTBOUND	65500	*	*	*	*	*	DENY

Design considerations

Description	Default Limit	Implications
Number of NSGs you can associate to a subnet, VM, or NIC	1	This means you cannot combine NSGs. Ensure all the rules needed for a given set of resources are included in a single NSG.
NSGs per region per subscription	100	By default, a new NSG is created for each VM you create in the Azure portal. If you allow this default behavior, you will run out of NSGs quickly. Make sure you keep this limit in mind during your design, and separate your resources into multiple regions or subscriptions if necessary.
NSG rules per NSG	200	Use a broad range of IP and ports to ensure you do not go over this limit.

Inter-Site Connectivity

Inter-Site Connectivity Options



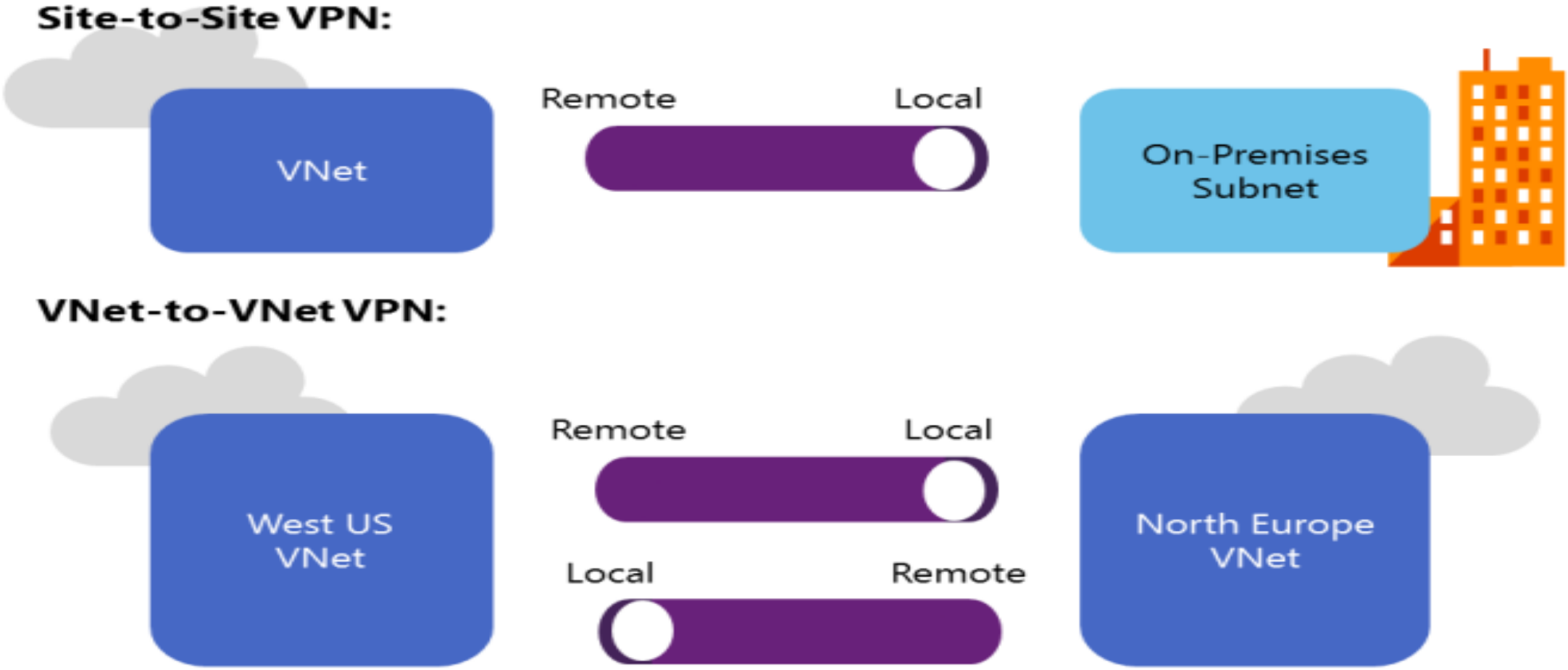
Configuring a Point-to-Site VPN

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 to the VPN.

Configuring a Site-to-Site VPN

1. Create a new custom Vnet.
2. Set local network values.
3. Set the VNet IP address spaces and subnets.
4. Create the virtual gateway.
5. Obtain VPN device configuration information.
6. Run the configuration script for the VPN gateway device.

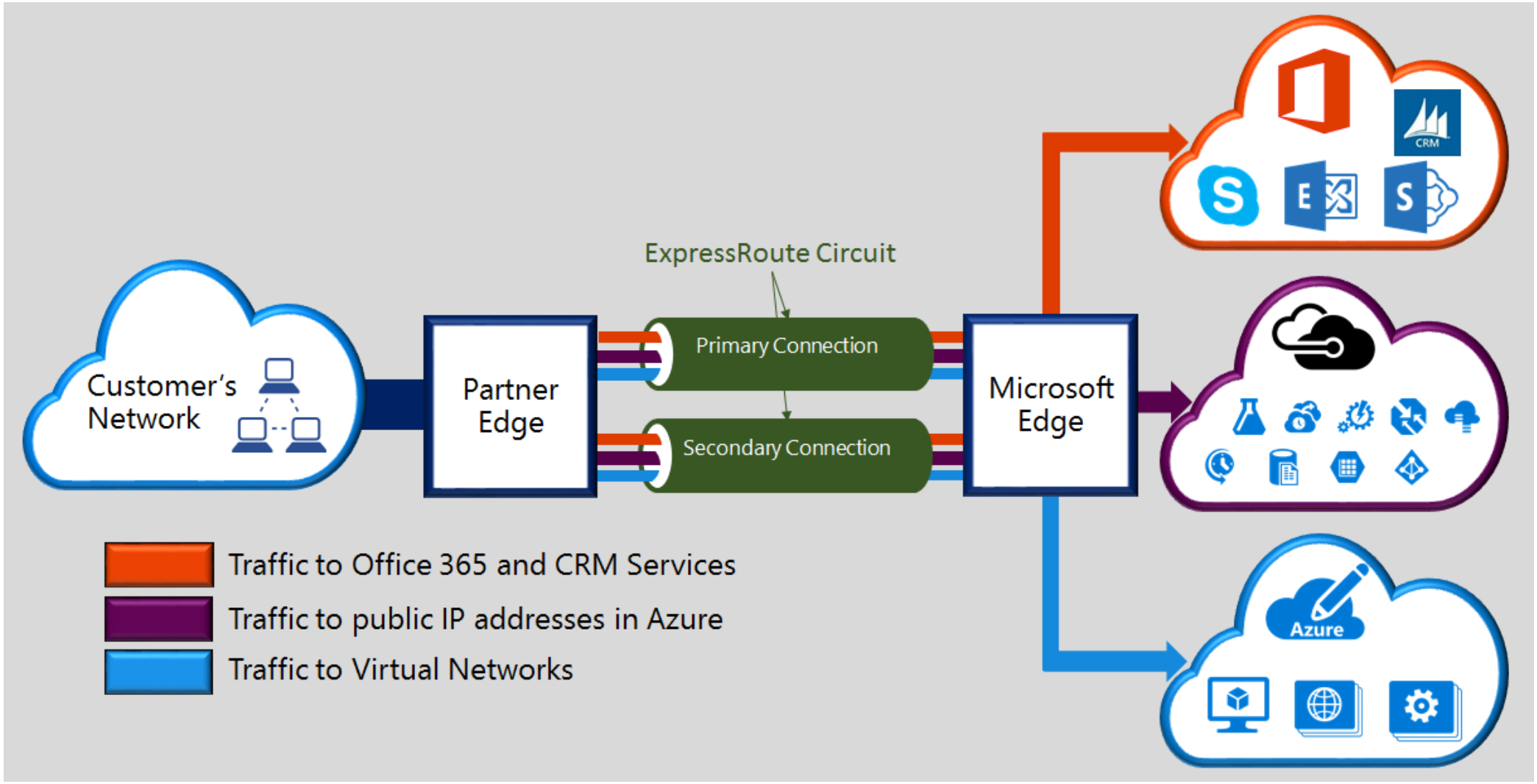
VNet-to-VNet connectivity



Configuring a VNet-to-VNet VPN

1. Create two VNets
   - Do not enable point-to-site or site-to-site communication
   - Ensure IP addresses do not overlap.
2. Add each VNet as a local network to the opposite VNet
   - Use a dummy IP address for the gateway address.
3. Create dynamic routing virtual gateways for each Vnet.
4. Substitute the real gateway IP addresses.
5. Connect the VPN gateways.

ExpressRoute



Demo