



AZ-300T04

Module 04: Configuring and Managing Virtual Networks

Ahmad Majeed Zahoory



1

Module 04: Configuring and Managing Virtual Networks

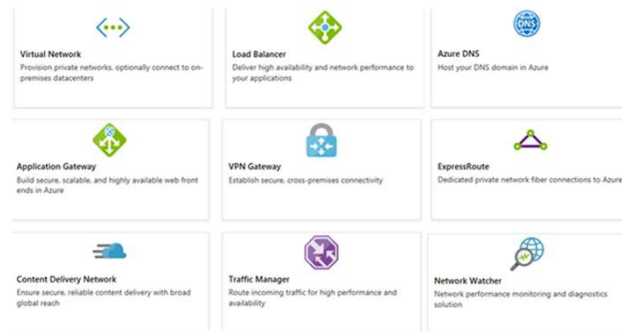
Lesson 01: Azure Virtual Networks



2

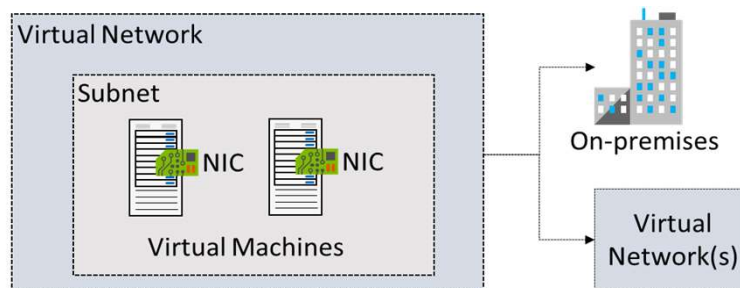
Azure Networking Components

- Adopting cloud solutions can save time and simplify operations
- Azure requires the same types of networking functionality as on-premises infrastructure
- Azure networking offers a wide range of services and products



3

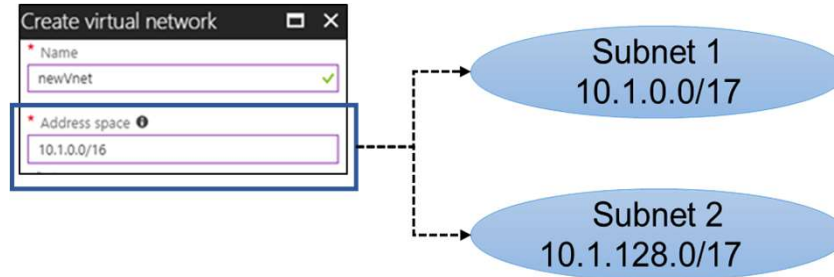
Virtual Networks



- Logical representation of your own network
- Create a dedicated private cloud-only VNet
- Securely extend your datacenter With VNets
- Enable hybrid cloud scenarios

4

Subnets



- A virtual network can be segmented into one or more subnets
- Subnets provide logical divisions within your network
- Subnets can help improve security, increase performance, and make it easier to manage the network
- Each subnet must have a unique address range - cannot overlap with other subnets in the virtual network in the subscription

5

Implementing Virtual Networks

- Create new virtual networks at any time
- Add virtual networks when you create a virtual machine
- Need to define the address space, and at least one subnet
- Be careful with overlapping address spaces

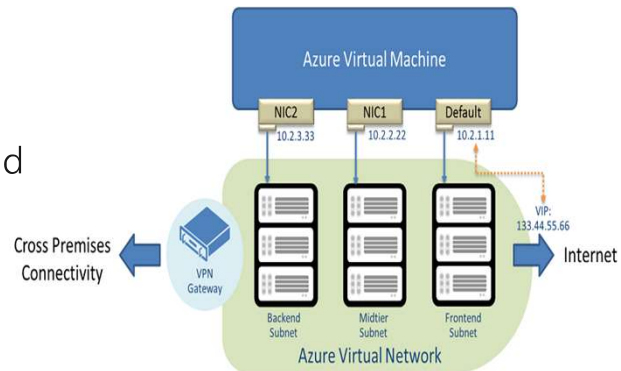
The screenshot shows the 'Create virtual network' dialog box with the following details:

- Name:** newVnet
- Address space:** 10.1.0.0/16
- Subnet:**
 - Name:** default
 - Address range:** 10.1.0.0/24 (10.1.0.0 - 10.1.0.255 (256 addresses))

6

Multiple NICs in Virtual Machines

- You can create virtual machines with multiple NICs
- Useful for virtual appliances, network traffic management, and isolation of traffic
- The VM size determines the number of NICs that can be supported



7

Module 04: Configuring and Managing Virtual Networks

Lesson 02: Review of IP Addressing



8

IP Addressing



- **Private IP addresses** are used within an Azure virtual network (VNet), and your on-premises network, when you use a VPN gateway or ExpressRoute circuit to extend your network to Azure
- **Public IP addresses** is used for communication with the Internet, including Azure public-facing services

9

Public IP Addresses

Public IP addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Load Balancer	Front-end configuration	Yes	Yes
VPN Gateway	Gateway IP configuration	Yes	No
Application Gateway	Front-end configuration	Yes	No

- A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways.

10

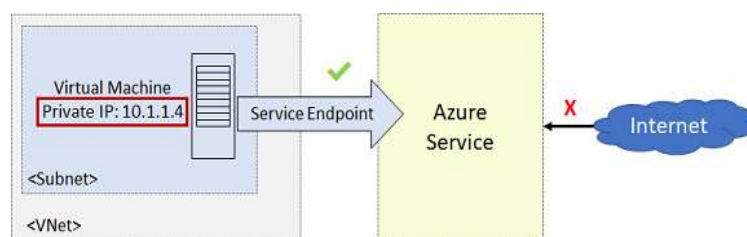
Private IP Addresses

Private IP Addresses	IP address association	Dynamic	Static
Virtual Machine	NIC	Yes	Yes
Internal Load Balancer	Front-end configuration	Yes	Yes
Application Gateway	Front-end configuration	Yes	Yes

- **Dynamic (default).** Azure assigns the next available unassigned or unreserved IP address in the subnet's address range
- **Static.** You select and assign any unassigned or unreserved IP address in the subnet's address range

11

Service Endpoints

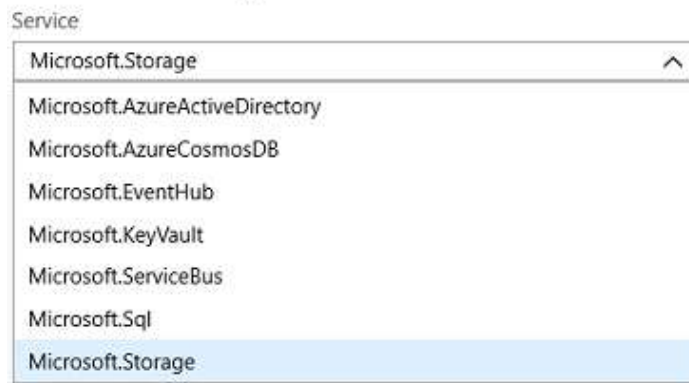


- Endpoints limit network access to specific subnets and IP addresses
- Improved security for your Azure service resources
- Optimal routing for Azure service traffic from your virtual network
- Endpoints use the Microsoft Azure backbone network
- Simple to set up with less management overhead

12

Service Endpoint Services

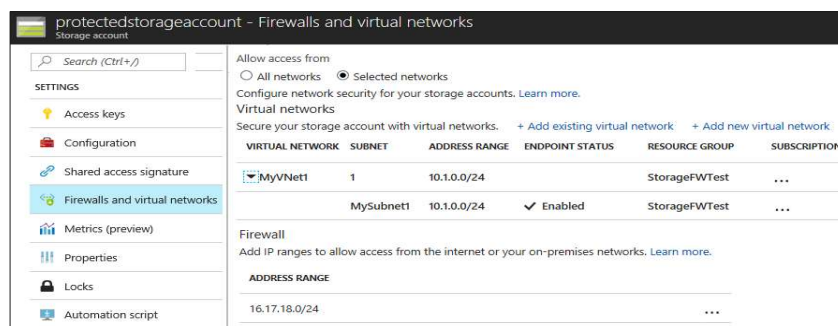
Add service endpoints



- ✓ Adding service endpoints can take up to 15 minutes to complete

13

Secure Access to Storage Endpoints



- Must configure both sides of the endpoints. For example, the virtual network side and the storage account side.
- Each service endpoint has its own Azure documentation page

14

Module 04: Configuring and Managing Virtual Networks

Lesson 03: Network Routing

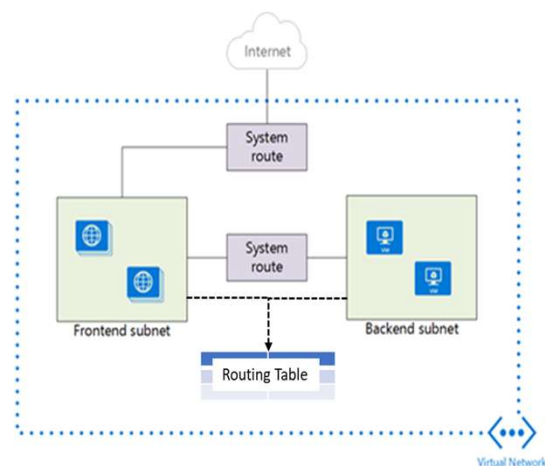


15

System Routes

System routes direct network traffic between virtual machines, on-premises networks, and the Internet

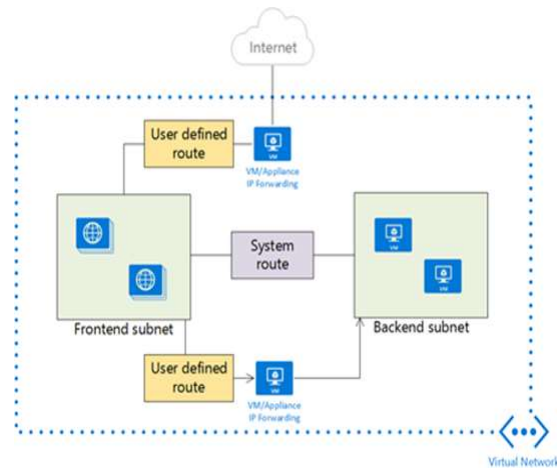
- Traffic between VMs in the same subnet
- Between VMs in different subnets in the same virtual network
- Data flow from VMs to the Internet
- Communication between VMs using a VNet-to-VNet VPN
- Site-to-Site and ExpressRoute communication through the VPN gateway



16

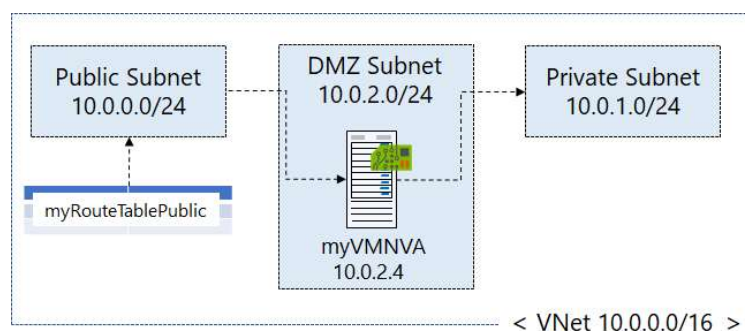
User Defined Routes

- A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network
- User-defined routes are custom routes that control network traffic by defining routes that specify the next hop of the traffic flow
- The next hop can be a virtual network gateway, virtual network, internet, or virtual appliance



17

Routing Example



1. Create a routing table
2. Create a custom route
3. Associate the route to the subnet

18

Create a Routing Table

- Border Gateway Protocol (BGP) is a standard routing protocol used to exchange routing and reachability information between two or more networks
- Routes are automatically added to the route table of all subnets with BGP propagation enabled
- In most situations you will want to enable BGP route propagation

Create route table
You can add routes to this table after it's created.

* Name: myRouteTablePublic ✓

* Subscription: Visual Studio Enterprise

* Resource group: ☐ Create new ☒ Use existing

* Location: West US

BGP route propagation:

19

Create a Custom Route

- When you create a route there are several Next hop types
- In this example, any private subnet IP addresses will be sent to the virtual appliance
- Other choices are Virtual network gateway, Virtual network, Internet, and None

Add route
cesrt

* Route name: ToPrivateSubnet ✓

* Address prefix ⓘ: 10.0.1.0/24 ✓

Next hop type ⓘ: Virtual appliance ^

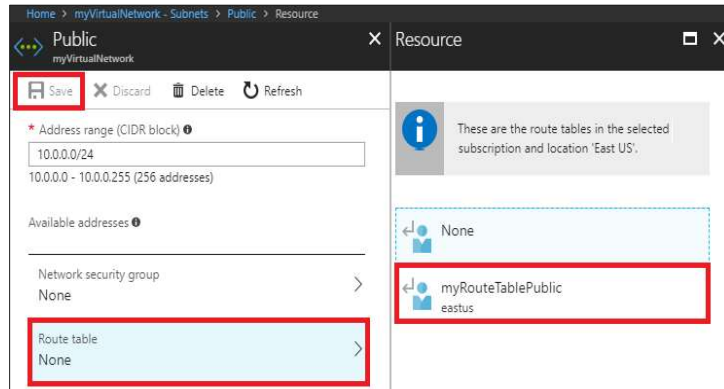
Virtual network gateway
Virtual network
Internet
Virtual appliance
None

* Next hop address ⓘ: 10.0.2.4 ✓

20

Associate the Route

- Each subnet can have zero or one route table associated to it
- In our example, the Public subnet will be associated with the routing table



21

Module 04: Configuring and Managing Virtual Networks

Lesson 04: Intersite Connectivity



22

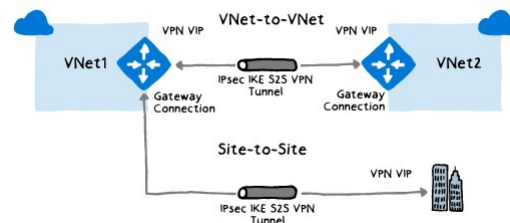
VNet-to-VNet Connections

Rely on VPN connectivity:

- **Require VPN gateways for each VNet**
- **Equivalent to Site-to-Site VPN in hybrid scenarios**

Support connecting:

- **VNets in the same or different regions.**
- **VNets in the same or different subscriptions.**
- **VNets and on-premises networks.**
- **ARM VNets and classic VNets.**

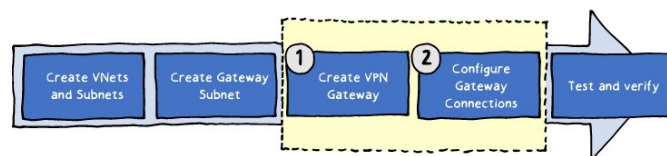


23

Implementing VNet-to-VNet VPN

Within each VNet:

- **Create the Gateway subnet**
- **Create a VPN gateway:**
 - **Name and Gateway Type**
 - **VPN Type**
 - **SKU**
 - **Virtual Networks**
 - **IP Address**



Create virtual network gateway

* Name

Gateway type ☒ VPN ☐ ExpressRoute

VPN type ☒ Route-based ☐ Policy-based

* Virtual network

* SKU

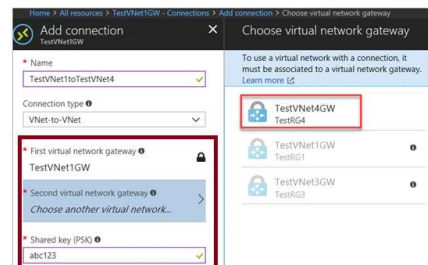
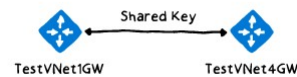
- Basic
- VpnGw1
- VpnGw2
- VpnGw3

* Public IP address ☒ Create new ☐ Use existing

24

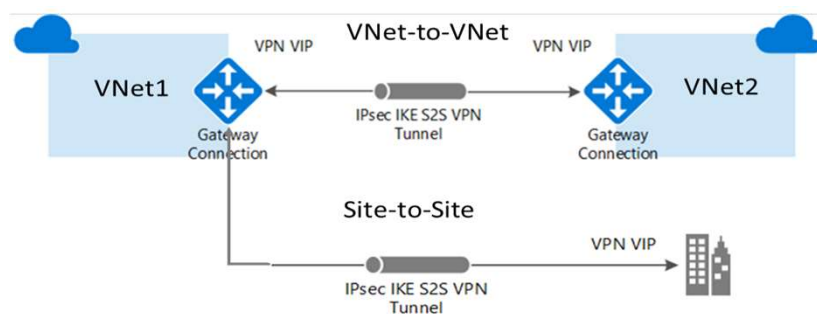
Configuring Gateway Connections

- The next step after provisioning of VPN gateways is completed
- Initial authentication is based on a shared key
- Implementation via:
 - **Azure PowerShell:**
 - For VNets in the same or different subscriptions
 - **The Azure portal:**
 - For VNets in the same subscription



25

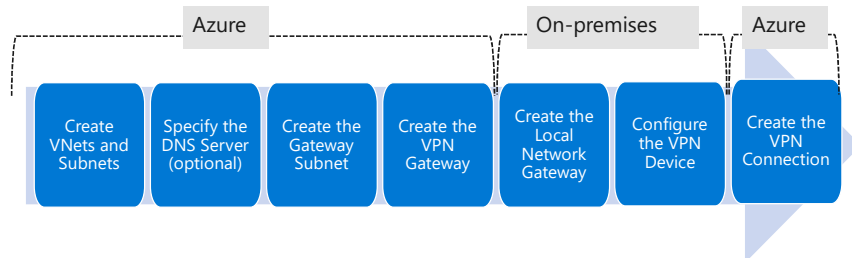
VNet-to-VNet Connections



- Connect VNets with a VNet-to-VNet VPN connection
- Requires a VPN gateway in each virtual network
- A secure IPsec/IKE tunnel provides the communication
- Use when VNet peering is not an option

26

Implement VNet-to-VNet Connections



- Take time to carefully plan your network configuration
- The on-premises part is necessary only if you are configuring Site-to-Site
- Always verify and test your connections

27

Create the Gateway Subnet

SETTINGS

<> Subnets

+ Subnet

+ Gateway subnet

search subnets

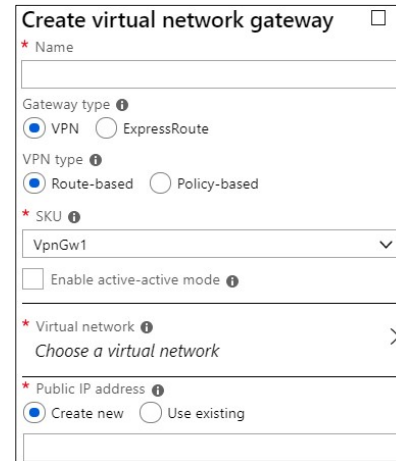
NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
default	10.1.0.0/24	251	-

- The gateway subnet contains the IP addresses; if possible, use a CIDR block of /28 or /27.
- When you create your gateway subnet, gateway VMs are deployed to the gateway subnet and configured with the required VPN gateway settings.
- Never deploy other resources (for example, additional VMs) to the gateway subnet.
- Avoid associating a NSG with the gateway subnet.

28

Create the VPN Gateway

- Use the VPN Gateway type
- Most VPN types are Route-based
- Your choice of gateway SKU affects the number of tunnels you can have and the aggregate throughput benchmark
- Associate a virtual network that includes the gateway subnet
- The gateway needs a public IP address



Create virtual network gateway ☐

* Name

Gateway type ⁱ

☒ VPN ☐ ExpressRoute

VPN type ⁱ

☒ Route-based ☐ Policy-based

* SKU ⁱ

VpnGw1

☐ Enable active-active mode ⁱ

* Virtual network ⁱ

Choose a virtual network

* Public IP address ⁱ

☒ Create new ☐ Use existing

✓ It can take up to 45 minutes to provision the VPN gateway

29

VPN Types

- Policy-based VPNs encrypt and direct packets through IPsec tunnels based on the IPsec policies
 - Can only be used on the Basic gateway SKU
 - You can have only 1 tunnel
 - You can only use Policy-based VPNs for S2S connections
- Route-based VPNs use *routes* in the IP forwarding or routing table to direct packets



Create virtual network gateway

VPN type ⁱ

☒ Route-based ☐ Policy-based

Most VPN Gateway configurations require a Route-based VPN

30

Gateway SKUs

SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2 Connections	Aggregate Throughput Benchmark
Basic	Max. 10	Max. 128	Not Supported	100 Mbps
VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps
VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps
VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps

✓ The Basic SKU is considered a legacy SKU

31

Create the Local Network Gateway

- Refers to the on-premises location
- Give the site a name by which Azure can refer to it
- The local gateway needs a public IP address
- Specify the IP address prefixes that will be routed through the gateway to the VPN device

Create local network gateway

* Name: VNet1LocalNet ✓

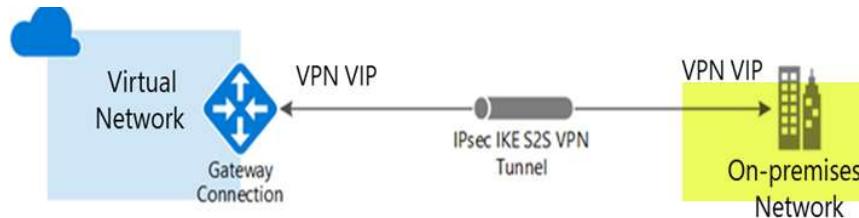
* IP address: 33.2.1.5 ✓

Address space: 192.168.3.0/24 ...

Add additional address range: ...

32

Configure the On-Premises VPN Device

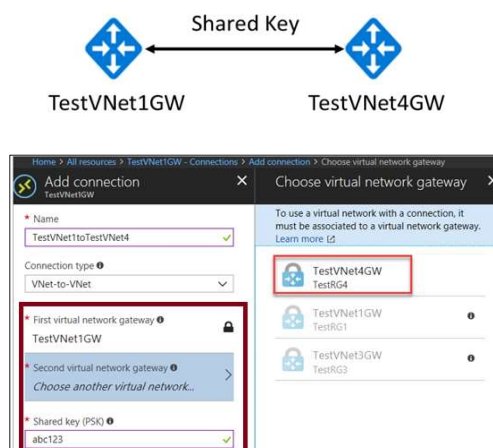


- Consult the list of supported VPN devices (Cisco, Juniper, Ubiquiti, Barracuda Networks)
- A VPN device configuration script may be available
- Remember the shared key for the Azure connection (next step)
- Specify the public IP address (previous step)

33

Create the VPN Connection

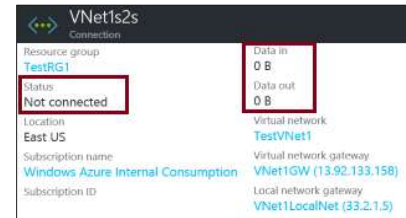
- Once your VPN gateways are created, you can create the connection between them.
- If your VNets are in the same subscription, you can use the portal.
- The shared key provides the connection
- Must create the connection for each virtual network



34

Verify the VPN Connection

- Azure Portal - Status should be Succeeded or Connected. Data should be flowing in the Data in and Data out information section.



- **PowerShell**

Verify the connection

```
Get-AzVirtualNetworkGatewayConnection -Name MyGWConnection -
ResourceGroupName MyRG
```

Review the status

```
"connectionStatus": "Connected",
"ingressBytesTransferred": 33509044,
"egressBytesTransferred": 4142431
```

35

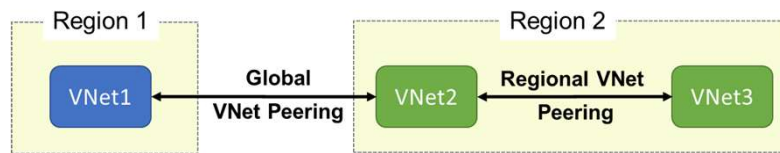
Module 04: Configuring and Managing Virtual Networks

Lesson 05: Virtual Network Peering



36

VNet Peering



- VNet peering connects two Azure virtual networks (not transient)
- Two types of peering: Regional and Global
- Peered networks use the Azure backbone for privacy and isolation
- Easy to setup, seamless data transfer, and great performance

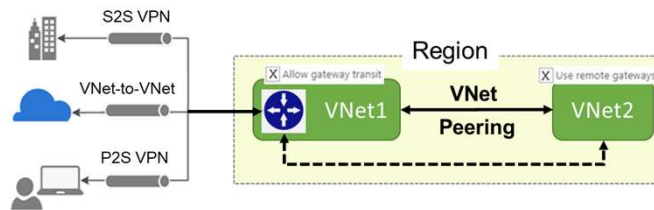
37

Configure VNet Peering

- **Allow forwarded traffic** - from within the peer virtual network into your virtual network
- **Allow gateway transit** - Allows the peer virtual network to use your virtual network gateway. (upcoming topic)
- **Use remote gateways** - only one virtual network can have this enabled

38

Gateway Transit



- Gateway transit allows peered virtual networks to share the gateway and get access to resources
- This means you do not need to deploy a VPN gateway in the peer virtual network

39

Global VNet Peering

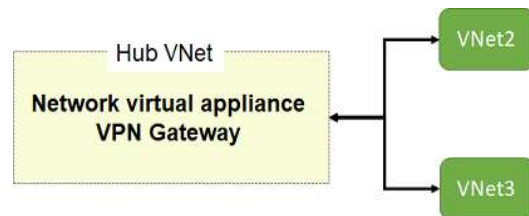
SETTINGS	NAME	PEERING STATUS	PEER	GATEWAY TRANSIT
<div> <div> DNS servers </div> <div> Peering </div> </div>	myVirtualNetwork1-myVirtualNetwork2	Initiated	myVirtualNetwork2	Disabled

- Global VNet peering connects virtual networks across regions
- Status will be Initiated or Connected
- Special requirements: public clouds only, virtual network resource limitations, no gateway transit, no transitivity, and limitations on high performance virtual machines.

40

Service Chaining

- Leverage user-defined routes and service chaining to implement custom routing
- Implement a VNet hub with a network virtual appliance or a VPN gateway
- Service chaining enables you to direct traffic from one virtual network to a virtual appliance, or virtual network gateway, in a peered virtual network, through user-defined routes



41

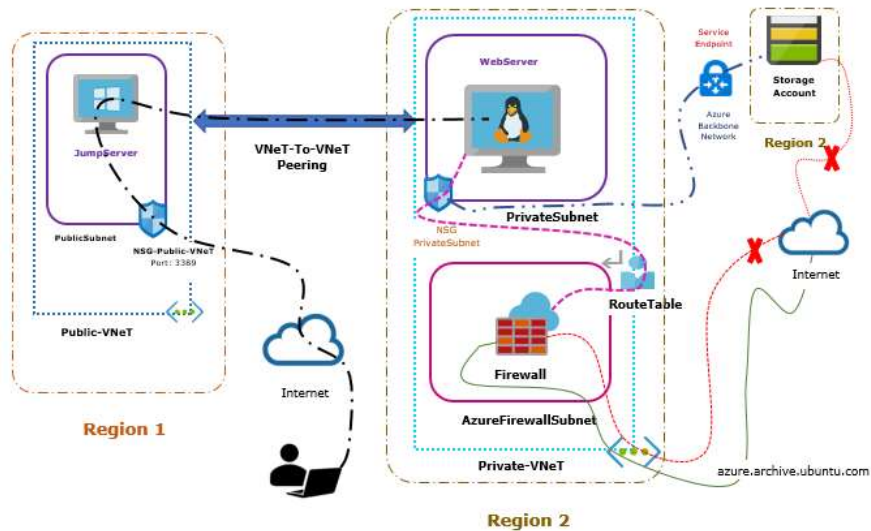
LAB [300TO01-M04-01]

1. Create Shared Services Network.



42

Part C



45

LAB [300TO01-M04-01]

1. Create Shared Services Network.

a. Services, Tools & Code used

- | | |
|----------------------------------|-----------------------------------|
| i. Azure Windows Virtual Machine | i. Azure Ubuntu Virtual Machine |
| ii. Azure Virtual Network | ii. Azure Virtual Network Peering |
| iii. Azure Subnet | iii. ARM Template |
| iv. Azure Network Security Group | iv. Azure PowerShell |
| v. Azure Storage | v. Custom Script Extension |
| vi. Azure Blob | vi. Bash Script |
| vii. Azure Firewall | |
| viii. Azure Route Table | |

Duration: 75 mnts.



46



47