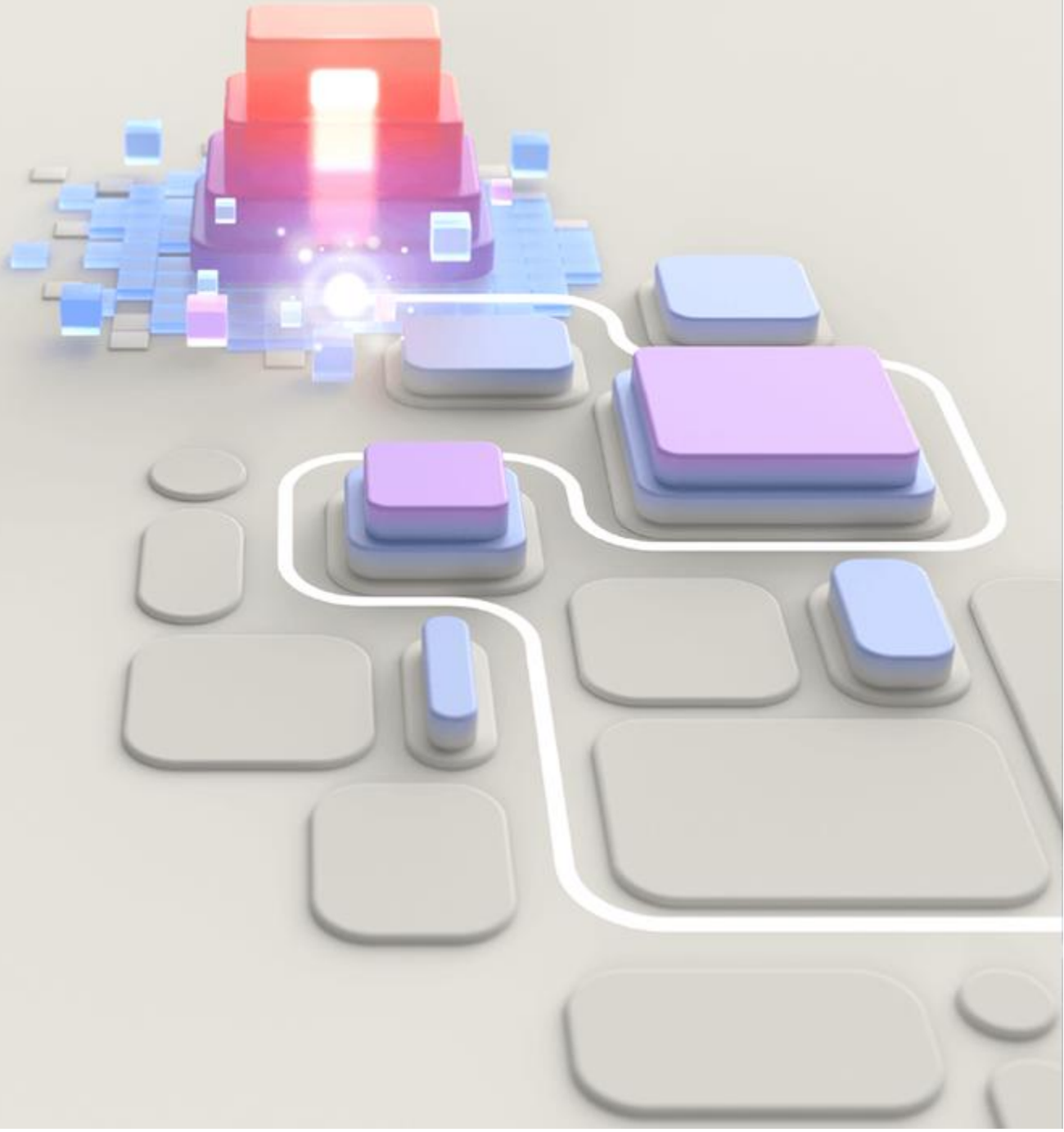
Microsoft

Azure
Implement & Manage



Berlin Physik

Thomas Jäkel

Azure 2016

Lead Trainer Cloud Infrastructure

Microsoft Certified Trainer since 1999

NT 4.0

AD

Bicep

AI

github.com/www42/aim

Azure - Implement & Manage (Applied Skills)

New
0 €

Certification
old
MCSE
169 €
Überwachung
theoretisch

LP
Lab

AZ-1002
Configure secure access to your workloads using Azure virtual networking

keine Überwachung
praktisch

LP
Lab

AZ-1003
Secure storage for Azure Files and Azure Blob Storage

"Assessment"
max 2h
Sprachen
72h

AZ-900
AZ-104

LP
Lab

AZ-1004
Deploy and configure Azure Monitor

LP

AZ-1007
Deploy and administer Linux virtual machines on Azure

Lab

Go Deploy

Microsoft Learn
Profile

Let’s get to know each other

9^00

15min

12^00 – 13^00

15min

17^00

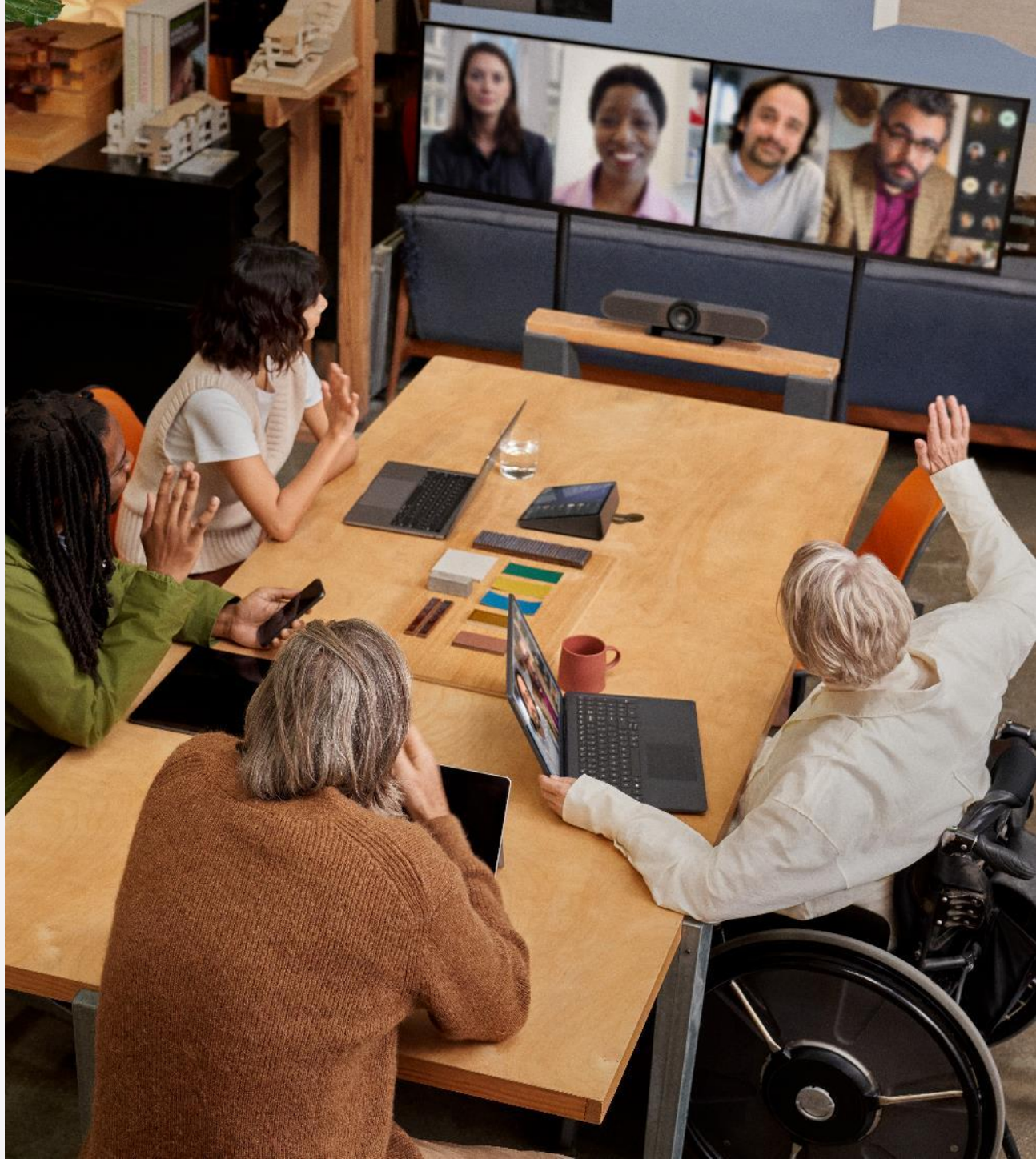
Your name

Company affiliation

Title/function

Your experience

Your expectations for the course



Get the most out of your Microsoft Learn profile

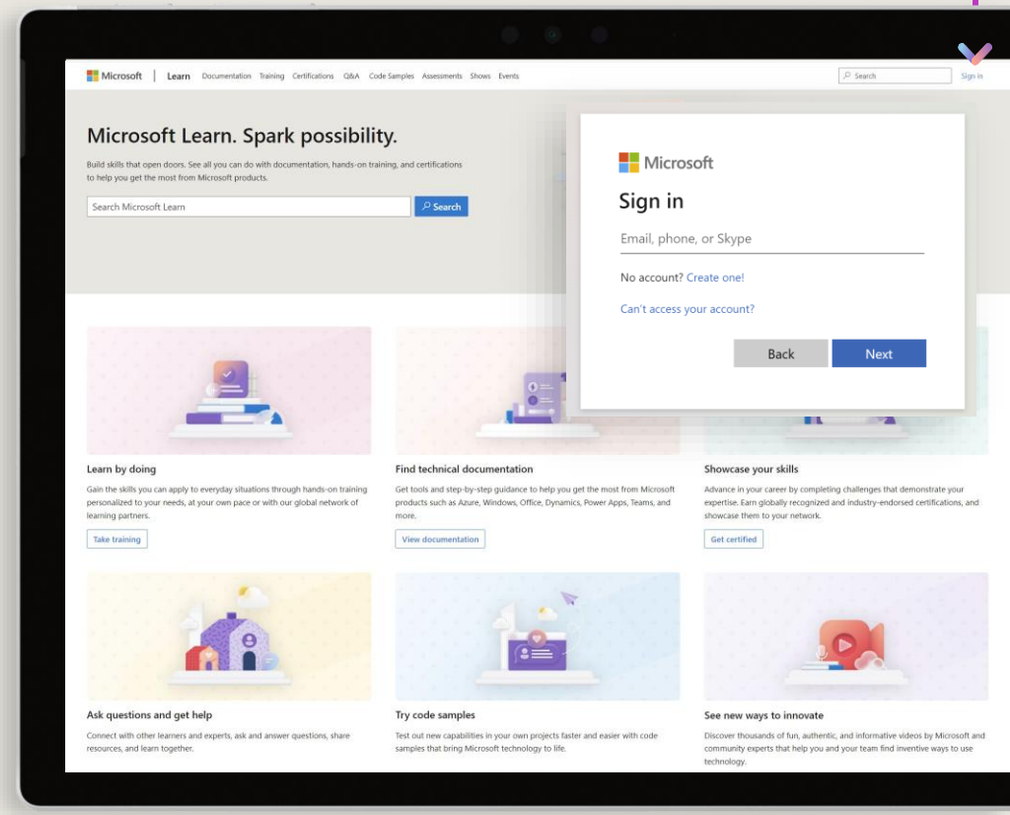
Verify, track, and share your training and certification progress and accomplishments—*all on one platform*

- Claim your achievement code for this course and share you have completed it.
- Access your course material and track progress on your learning activities.
- Share and verify your Microsoft Certifications via email, on social networking platforms, and on your résumé.
- Download and print transcripts and certificates.
- Manage your upcoming activities and certification exam appointments.

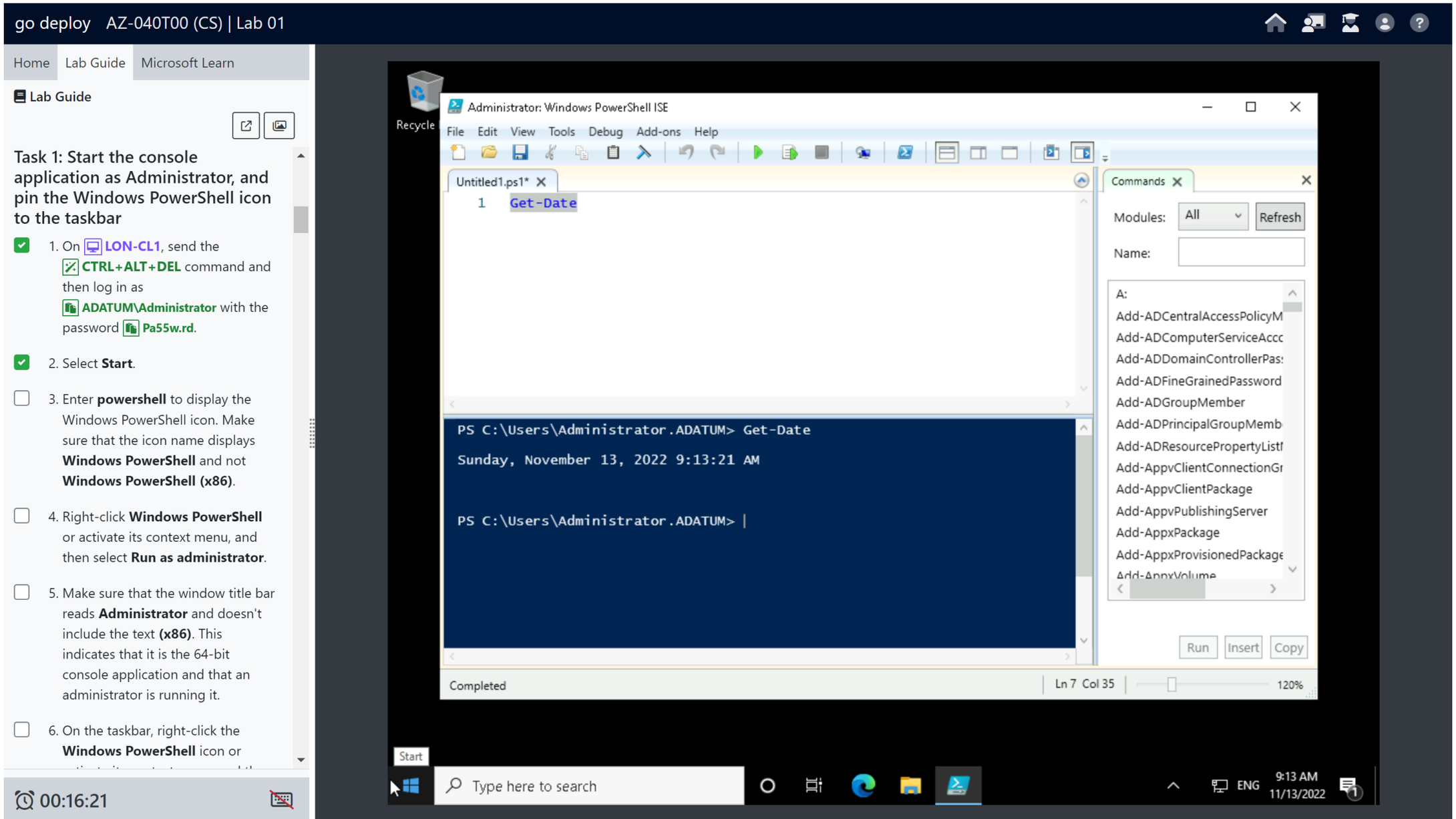
www.aka.ms/MyMicrosoftLearnProfile

Create your Microsoft Learn profile at learn.microsoft.com

- Select *Sign in* at the top, right corner of any Microsoft Learn page.
- Follow the Microsoft account authentication process.
- If the account that you have chosen to sign-in with doesn't already have a Microsoft Learn profile, you'll be guided to create one.



go deploy - Lab Umgebung



Microsoft

AZ-1002
Configure secure access to your workloads using Azure virtual networking

ID Provider Entra ID

M365

Lizenz E5

TAP

Paul

APP

Tenant

Azure

Role "owner"

Management Group(s)

Subscription 1 $

Sub 2 $

Sub 3 $

Resource Group 1

RG2 RG3

RG4

SA

VNet

Interface

VM

Introduction to the course scenario

Your organization is developing a new web application that will be hosted on Azure. Leadership has determined that they will adopt the Enterprise Scale Azure Landing Zone in phases to start with a strong cloud foundation and support the new web app. As the Azure Administrator your help is needed to ensure that the appropriate networking infrastructure is deployed as they begin phase one.

- Provide a shared services virtual network with network isolation and segmentation for the web application.
- Control the network traffic to and from the web application.
- Protect the web application from malicious traffic and block unauthorized access.
- Route traffic to the Firewall.
- Record and resolve domain names internally.

NSG ASG

VM App :443

vnet

DNS private zone

Link

www A 10.0.0.4

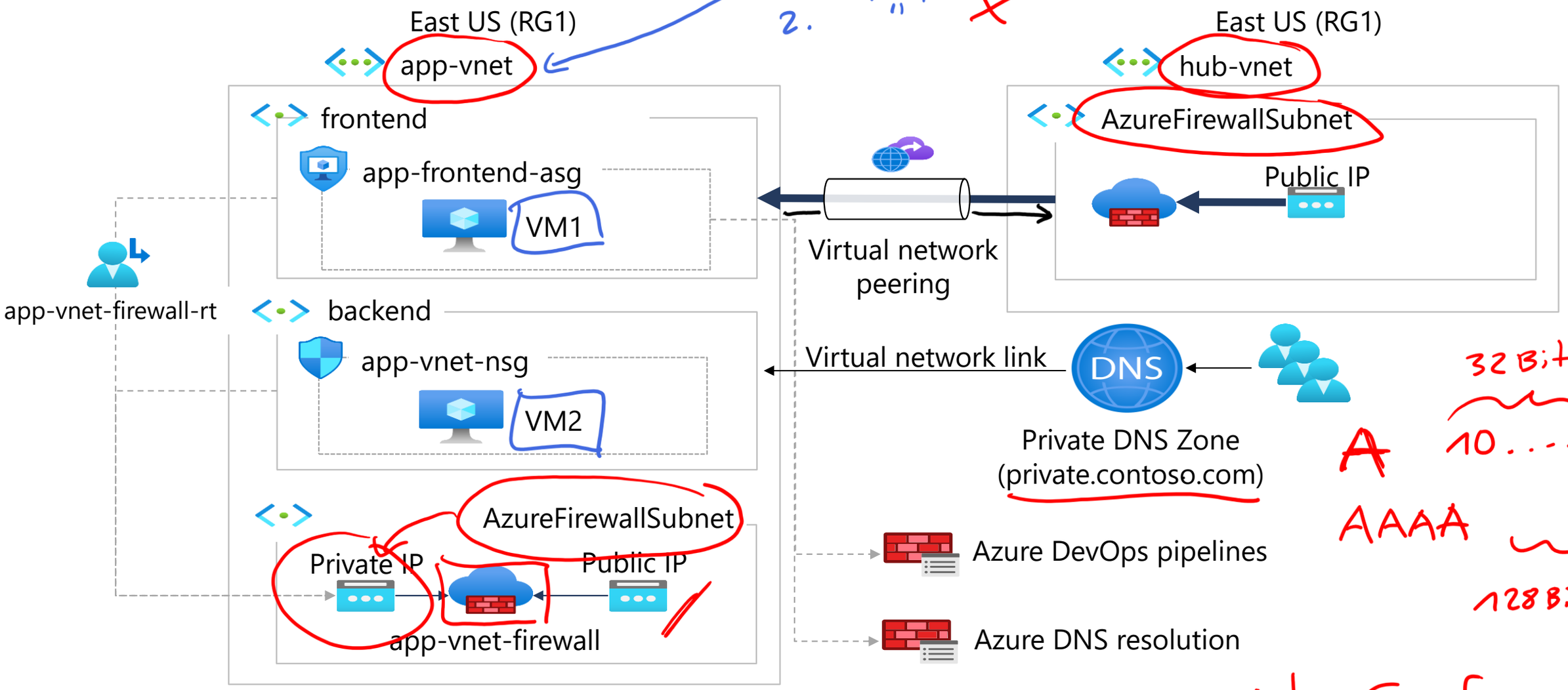
TCP/IP :443

Completed architecture diagram

Bicep Template (idempotent)

New-AzVirtualNetwork

1. Deployment
2. "



32 Bit

A 10....

AAAA

128 Bit

Vint Cerf

TCP/IP 1962

Create and configure virtual networks

Agenda: Virtual networks and peering

- Capabilities of Azure Virtual Networks
- Instructor demonstration
  - What are subnets and how many do you need?
  - What is VNet peering?
- Student exercise: Create and configure virtual networks
- Review questions and reference module

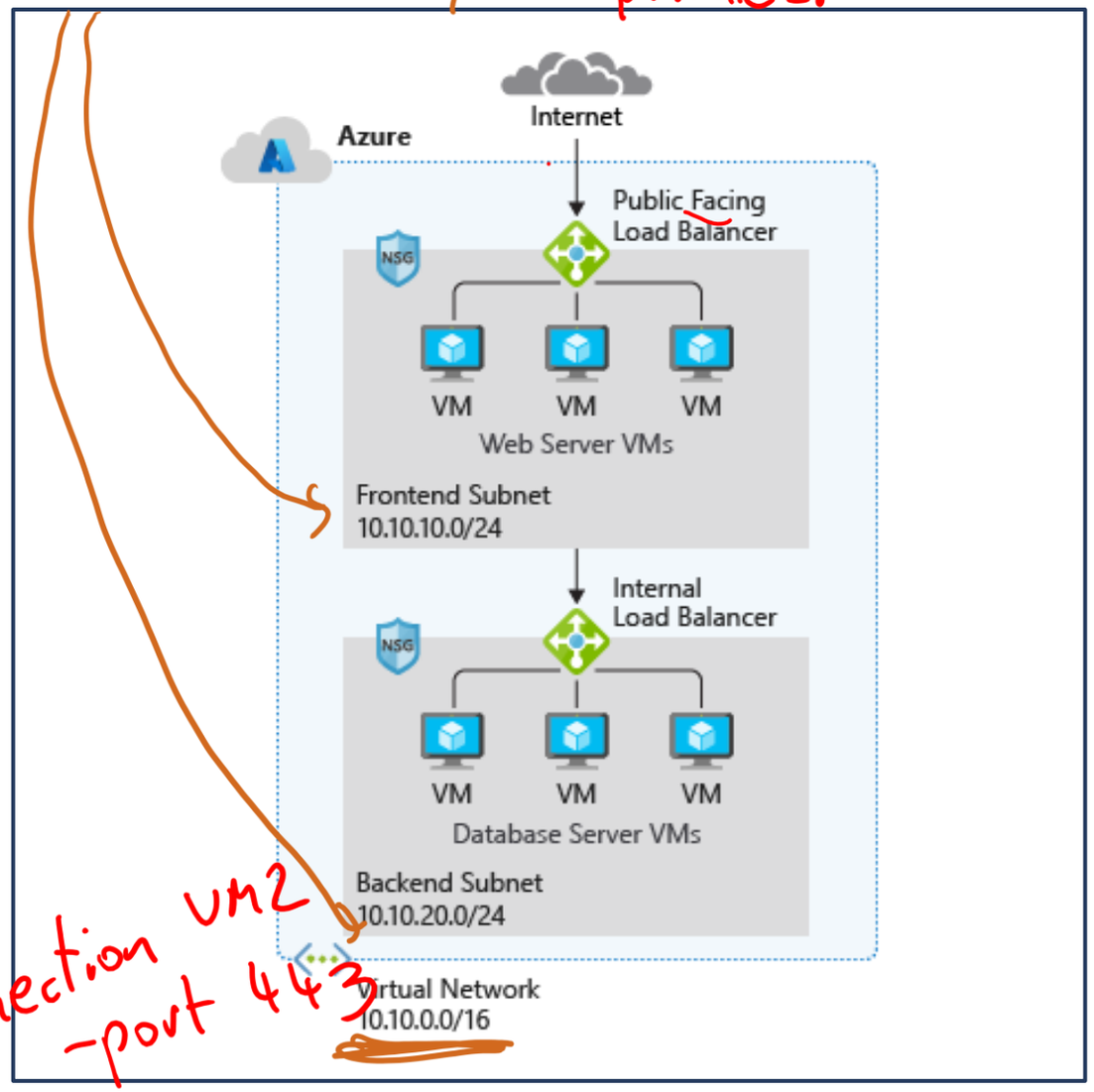
Terraform → Azure Resource Manager ARM
Bicep →

Capabilities of Azure Virtual Networks

VM Interface VM2 SA

VNet 10.10.0.0/16 private EP Interface

- Communication with the Internet
- Communication between Azure resources
- Communication between on-premises resources
- Filtering network traffic
- Routing network traffic



Test-Netconnection VM2 -port 443

Demo 01 – Virtual Networks

- Create a virtual network in the Azure portal
- Configure subnets
- Peer two virtual networks

Create Subnets

+ Subnet | + Gateway subnet | Refresh | Manage users | Delete

Name	IPv4	IPv6	Available IPs	Delegated
subnet0	10.0.0.0/24	-	250	-
subnet1	10.0.1.0/24	-	251	-
subnet2	10.0.2.0/24	-	251	-
AzureBastionSubnet	10.0.30.0/26	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

VM

BH

VPN GW

Azure FirewallSubnet

A virtual network can be segmented into one or more subnets

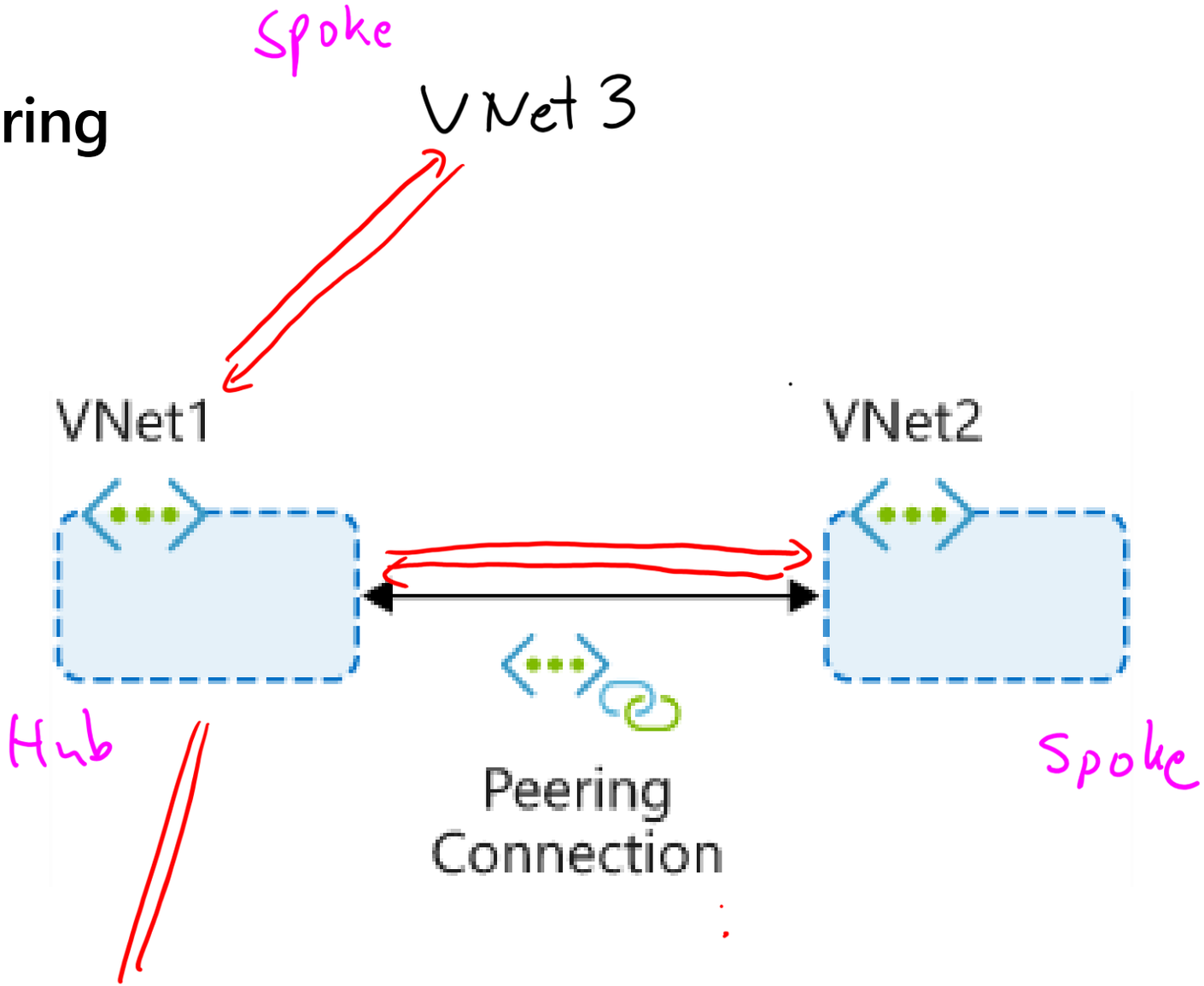
Subnets provide logical divisions within your network

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 VNet in the subscription

Configure virtual network peering

- Two types of peering: Global and Regional
- Connects two Azure virtual networks
- Ability to peer across subscriptions and tenants
- Peered networks use the Azure backbone for privacy and isolation
- Easy to setup, seamless data transfer, and great performance



Review and reference – Virtual networks and peering

Check your knowledge questions and additional study

What is a virtual network and what things should you consider when creating a virtual network?

What is VNet peering and why would use it?

MODULE

Configure Azure Virtual Network peering

41 min

Azure • Administrator • Intermediate

MODULE

Configure virtual networks

35 min

Azure • Administrator • Intermediate

Microsoft

Paket- Filter
Header

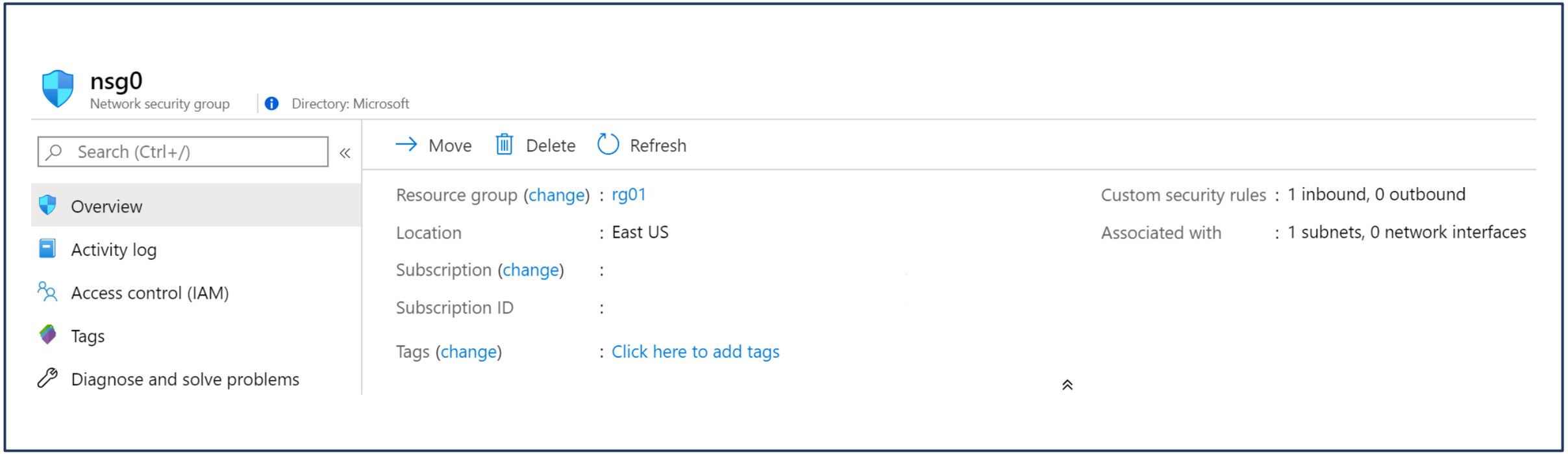
Create and configure NSG and ASG

"Label"
"web-Server"

Agenda: Security Groups

- What is a Network Security Group (NSG)?
- Instructor Demonstration
  - Determine NSG Rules
  - Implement Application Security Groups
- Student Exercise: Create and configure NSGs
- Review questions and reference module

What is a Network Security Group?



Limits network traffic to resources in a virtual network

Lists the security rules that allow or deny inbound or outbound network traffic

Associated to a subnet or a network interface

Can be associated multiple times

Demo 02: Network and Application Security Groups

- Create a Network Security Group
- Explore inbound and outbound rules
- Create an Application Security Group
- Associate the NSG

Determine NSG Rules

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	RDP_Inbound	3389	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces

There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

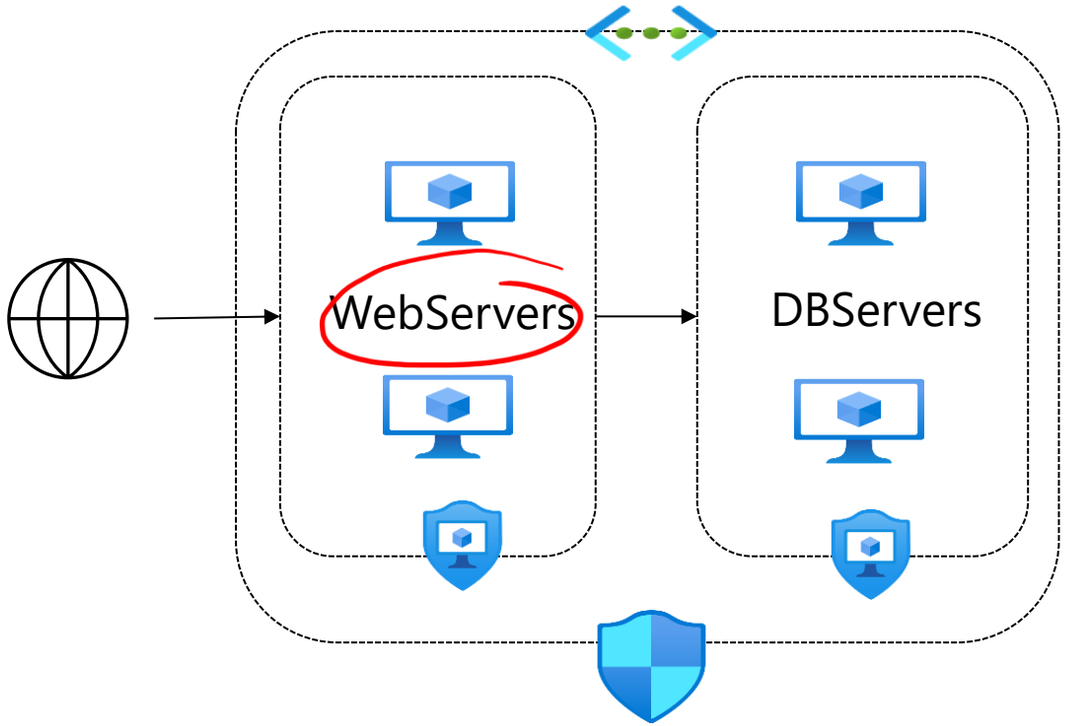
Implement Application Security Groups

Extends your application's structure

ASGs logically group virtual machines – web servers, application servers

Define rules to control the traffic flow

Wrap the ASG with an NSG for added security



Source	Destination	Port
Internet	WebServers	80, 443
WebServers	DBServers	1433

Exercise 02: Create and configure network security groups

Your organization requires the network traffic in the app virtual network to be tightly controlled.

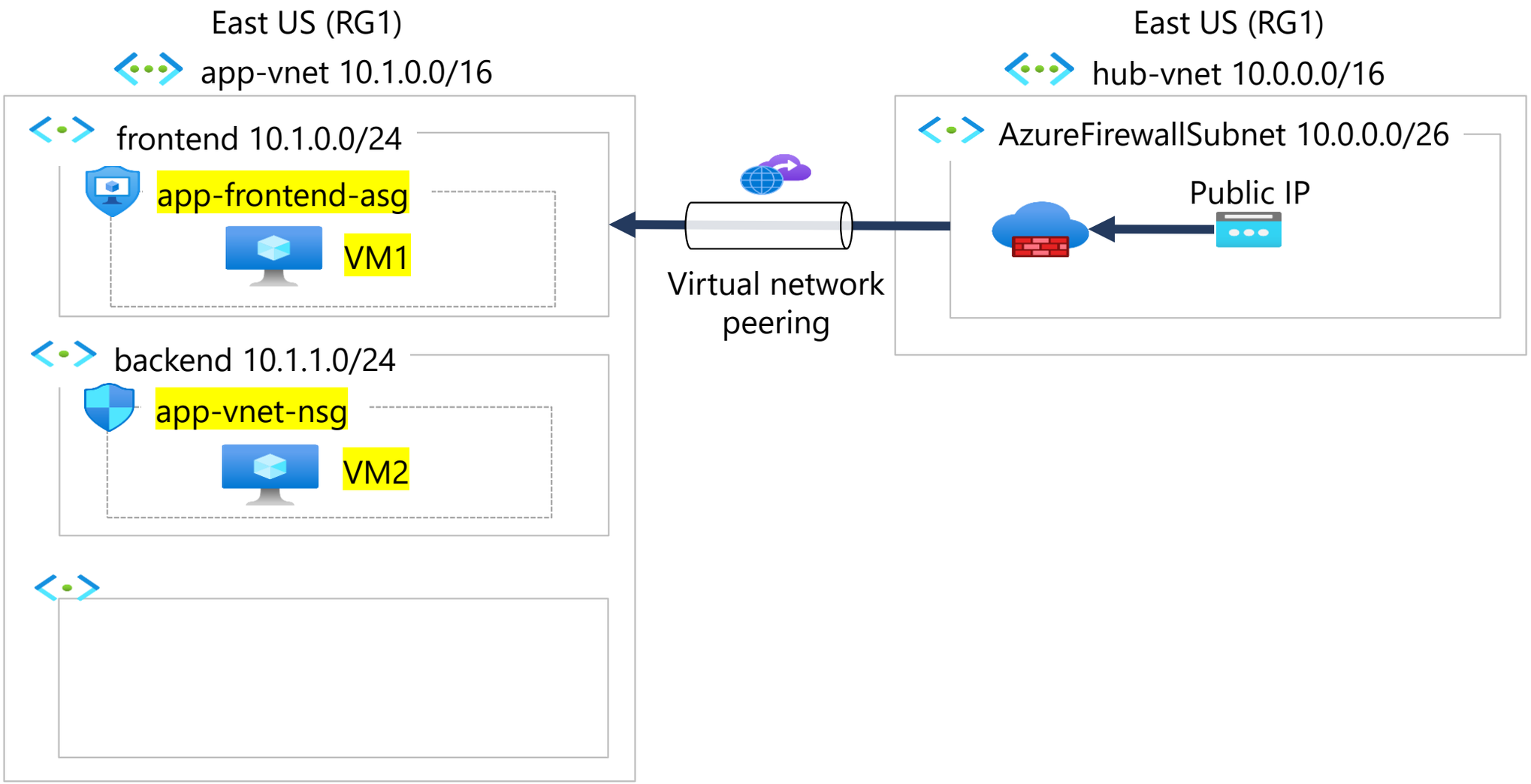
- The frontend subnet has web servers that can be accessed from the internet. An application security group (ASG) is required for those servers.
- An NSG rule is required to allow inbound HTTPS traffic to the ASG. This rule uses the TCP protocol on port 443.
- The backend subnet has database servers used by the frontend web servers. A network security group (NSG) is required to control this traffic.
- An NSG rule is required to allow inbound network traffic from the ASG to the backend servers. This rule uses the MS SQL service and port 1443.

Skilling tasks:

- ❑ Create an NSG.
- ❑ Associate an NSG to a subnet or a network interface.
- ❑ Create NSG security rules.
- ❑ Create and use Application Security Groups (ASGs) in NSG security rules.

Architecture diagram

Exercise 02: Create and configure network security groups



Review and reference – NSG and ASG

Check your knowledge questions and additional study

What is a network security group and when would you use it?

What is an application security group and when would you use it?

MODULE

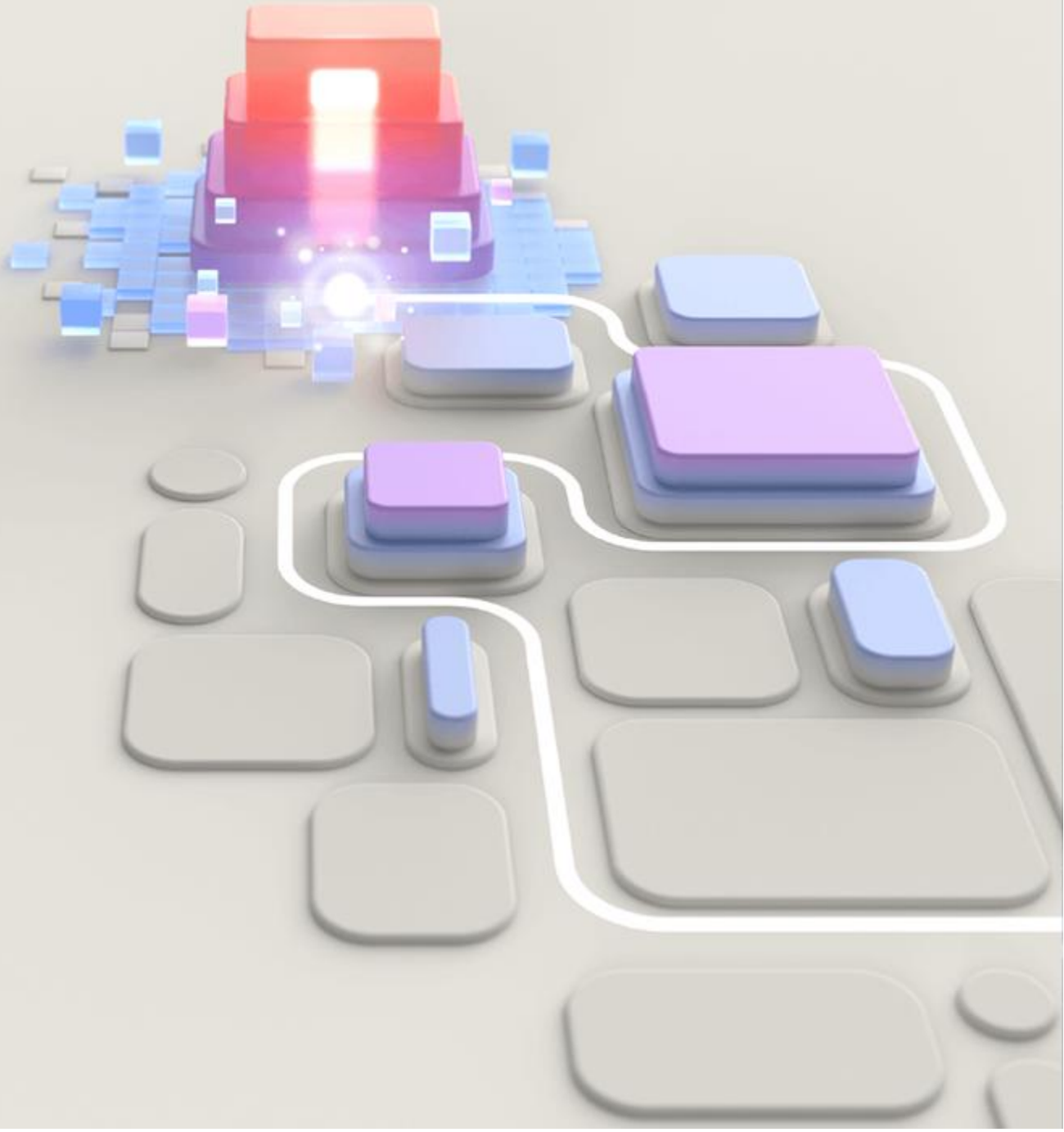
Configure network security groups

36 min

Azure • Administrator • Intermediate

Microsoft

Create and configure Azure Firewall



Agenda: Azure Firewall & Firewall Policy

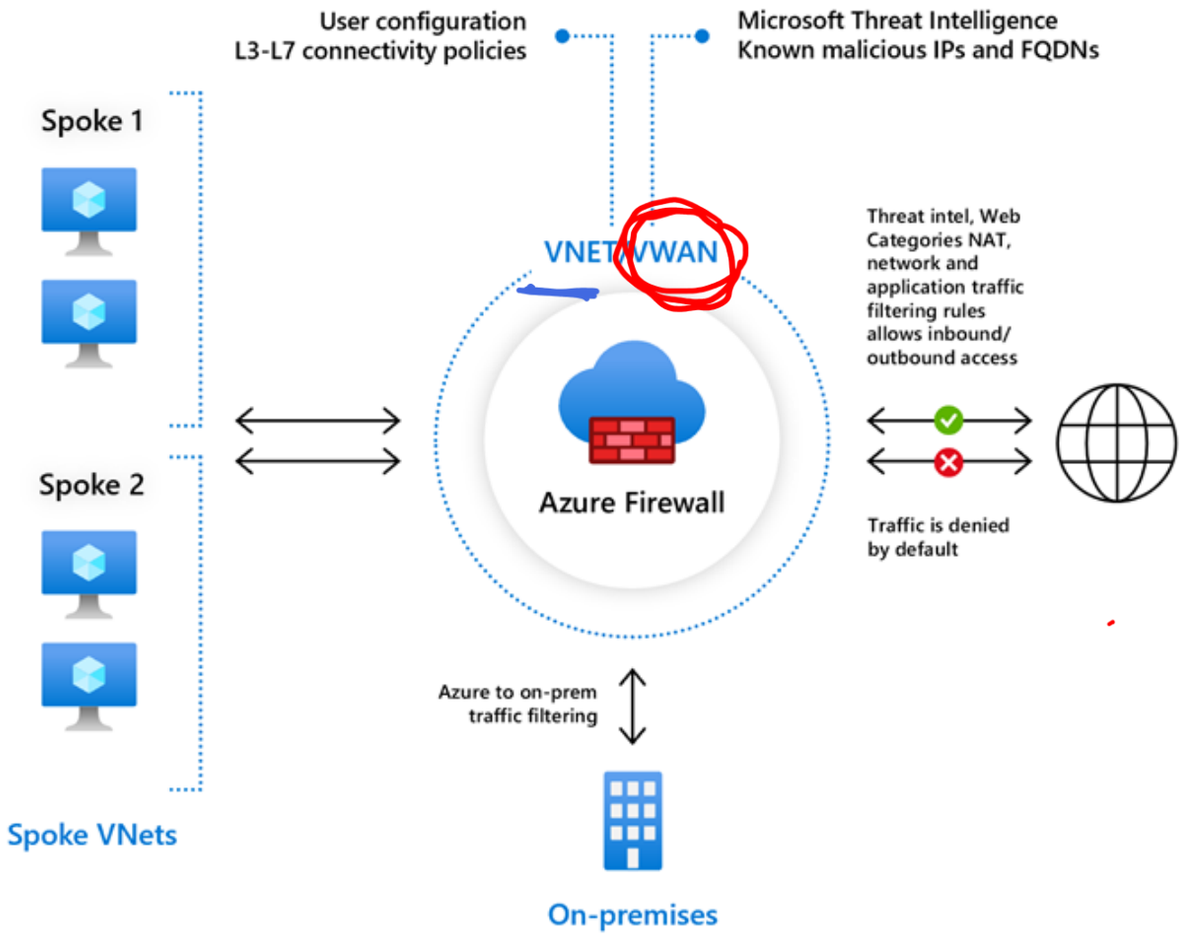
- What is Azure Firewall?
- Instructor demonstration
  - What is Azure Firewall Policy?
- Student exercise: Create and configure Azure Firewall
- Review questions and reference module

UDR

WAF HTTPS
App GW
Front Door

What is Azure Firewall?

- Stateful firewall as a service
- Built-in high availability
- Managed with policies
- Threat intelligence-based filtering
- Fully integrated with Azure Monitor
- Support for hybrid connectivity



Demo 03: Azure Firewall & Azure Firewall Policy

- Create an Azure Firewall
- Create Firewall Policy
- Create rules within Firewall Policy

Create Azure Firewall Rules

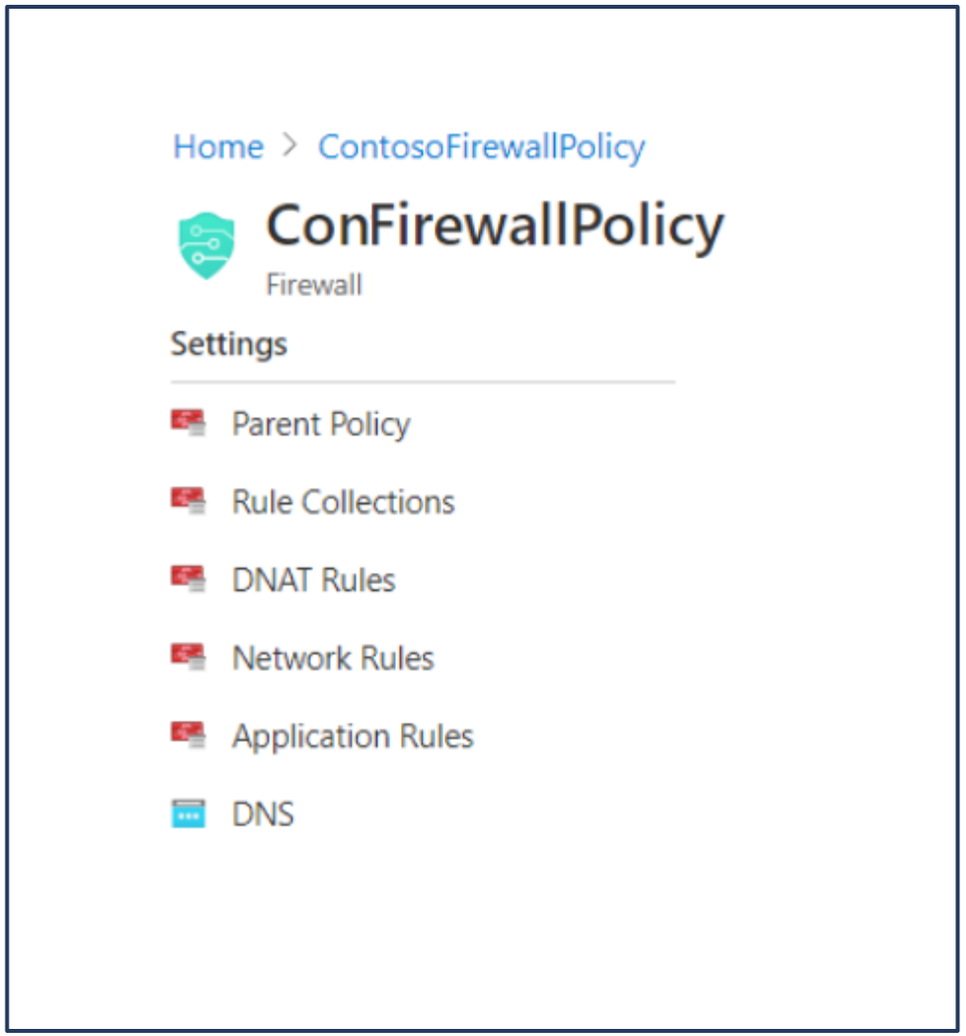
Azure Firewall Manager centralizes firewall management

Firewall policies container rules and settings to control access:

1 • **NAT rules** allow incoming connections

2 • **Network rules** contain source and destination addressed, protocol, and destination ports

3 • **Application rules** provide qualified domain name (FQDNs) that can be access from a subnet



Exercise 03: Create and configure Azure Firewall

Your organization requires centralized network security for the application virtual network. As the application usage increases, more granular application-level filtering and advanced threat protection will be needed. Also, it is expected the application will need continuous updates from Azure DevOps pipelines.

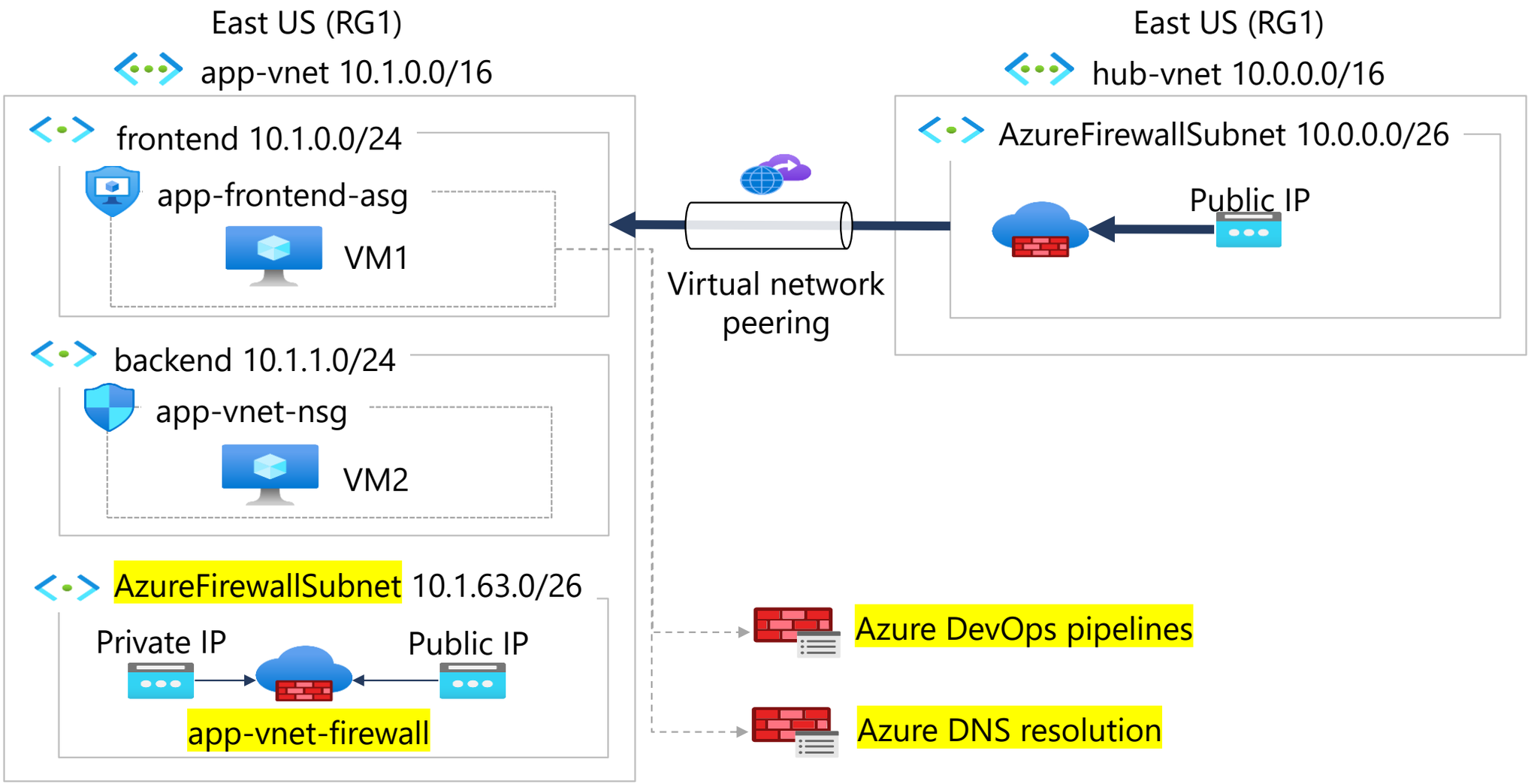
- Azure Firewall is required for additional security in the app-vnet.
- A firewall policy should be configured to help manage access to the application.
- A firewall policy application rule is required. This rule will allow the application access to Azure DevOps so the application code can be updated.
- A firewall policy network rule is required. This rule will allow DNS resolution.

Skilling tasks:

- ❑ Create an Azure Firewall.
- ❑ Create and configure a firewall policy.

Architecture diagram

Exercise 03: Create and configure Azure Firewall



Review and reference – Azure Firewall & Policy

Check your knowledge questions and additional study

What is Azure Firewall and how do you use it?

What is Azure Firewall Policy?

MODULE

Introduction to Azure Firewall

48 min

Azure • Administrator • Beginner

Microsoft

UDR

NVA

Route Table

Appliance

Configure network routing

(BGP)

Agenda: Network routing

- Instructor demonstration
  - Review System Routes
  - Identify User-Defined Routes
- Student exercise: Configure network routing
- Review questions and reference module

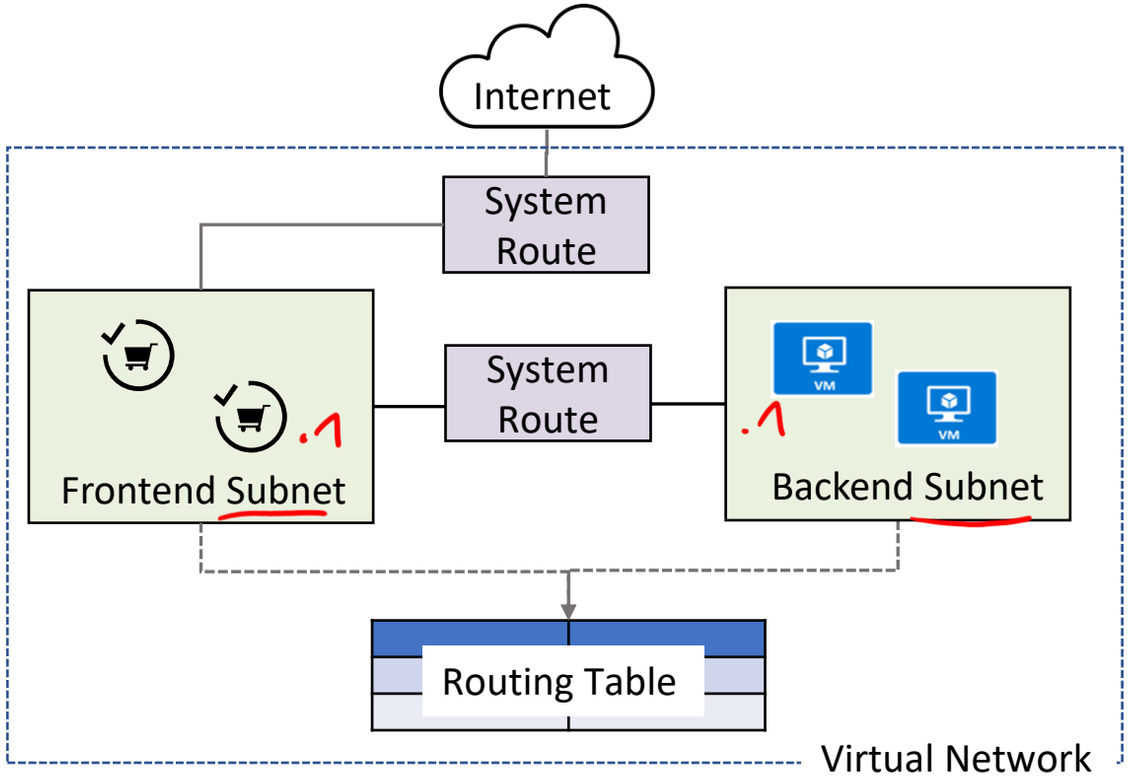
Demo 04: Route tables

- Create a Route Table
- Create a route in the route table
- Associate the route table to a subnet

Review 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

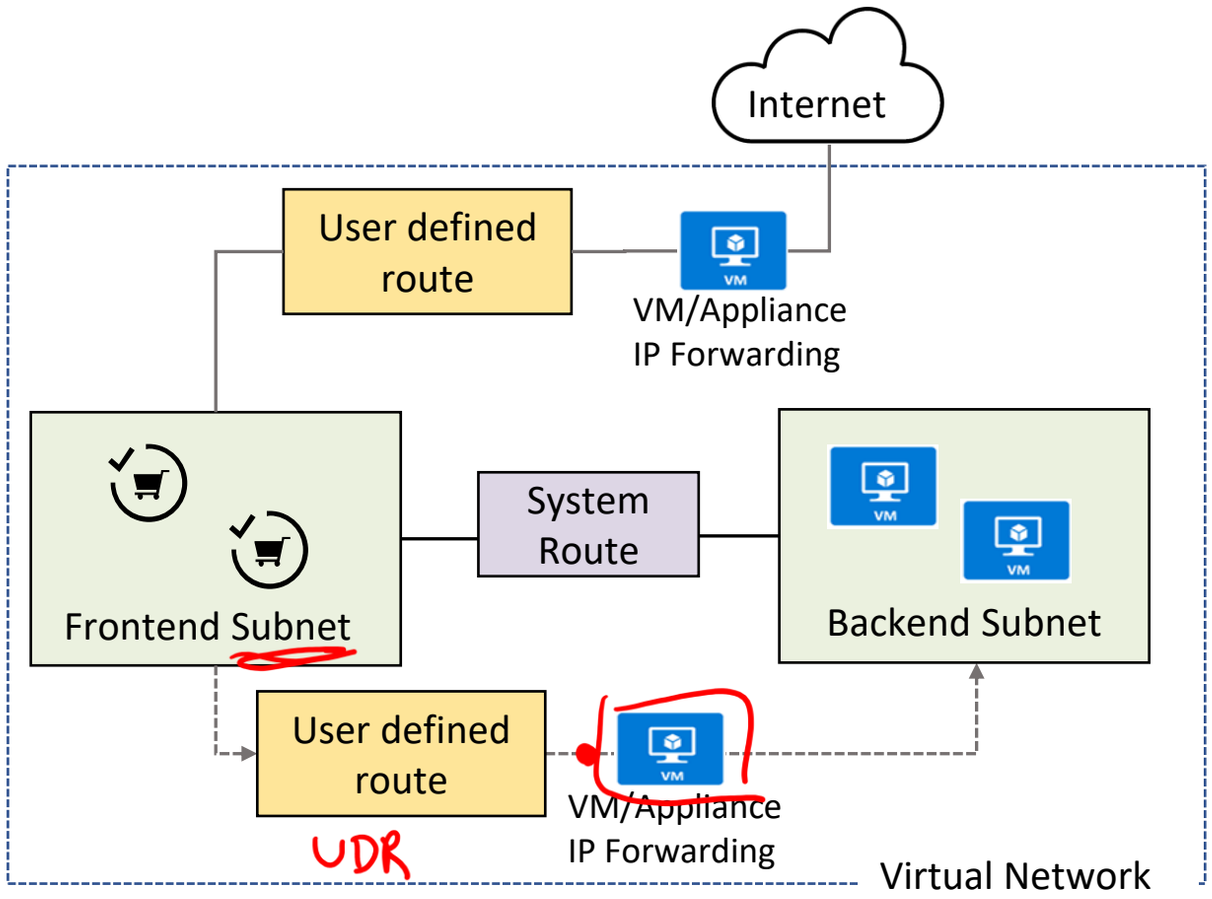


Identify User-Defined Routes

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



Exercise 04: Configure network routing

To ensure the firewall policies are enforced, outbound application traffic must be routed through the firewall.

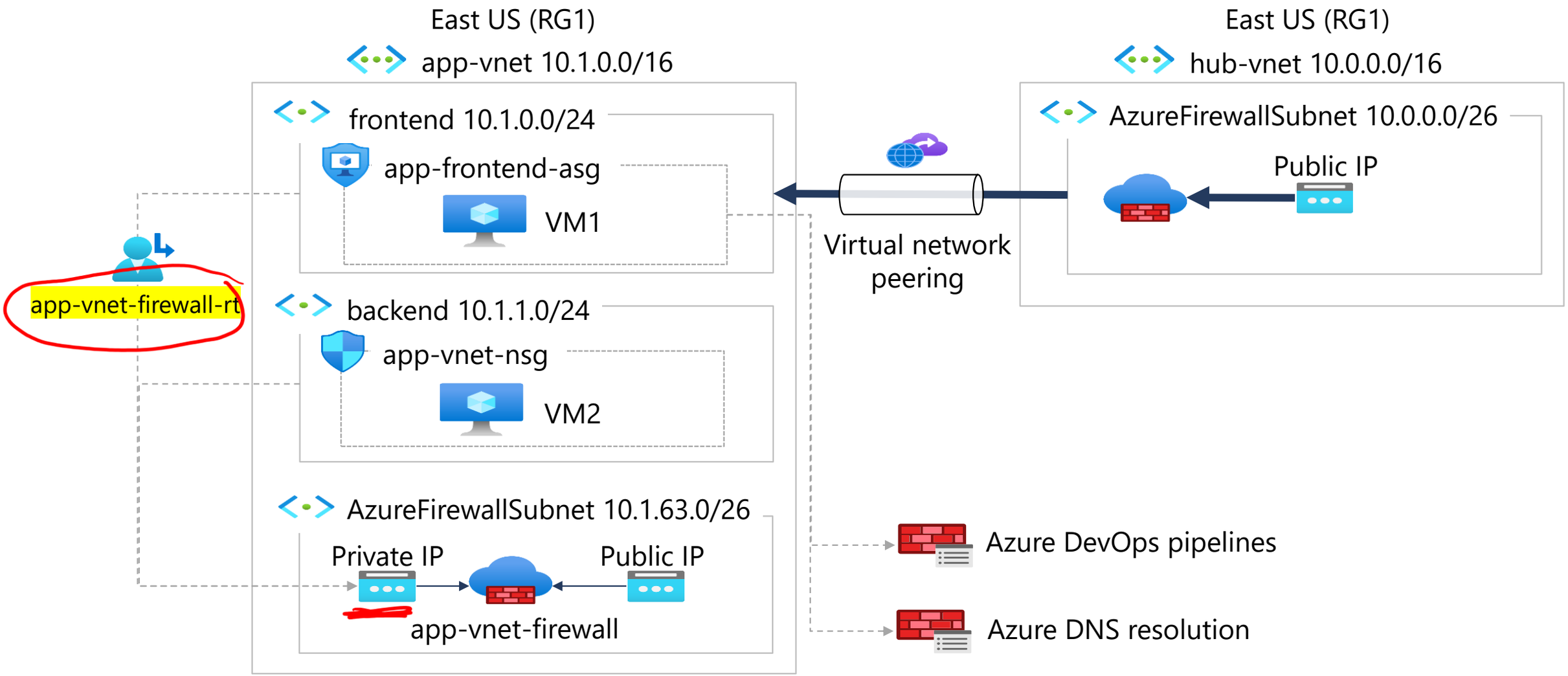
- A route table is required. This route table will be associated with the frontend and backend subnets.
- A route is required to filter all outbound IP traffic from the subnets to the firewall. The firewall's private IP address will be used.

Skilling tasks:

- ❑ Create and configure a route table.
- ❑ Associate a route table to a subnet.

Architecture diagram

Exercise 04: Architecture diagram



Review and reference – Routing

Check your knowledge questions and additional study

What is the difference between system-defined routes and user-defined routes?

Why would you use a custom route in a virtual network?

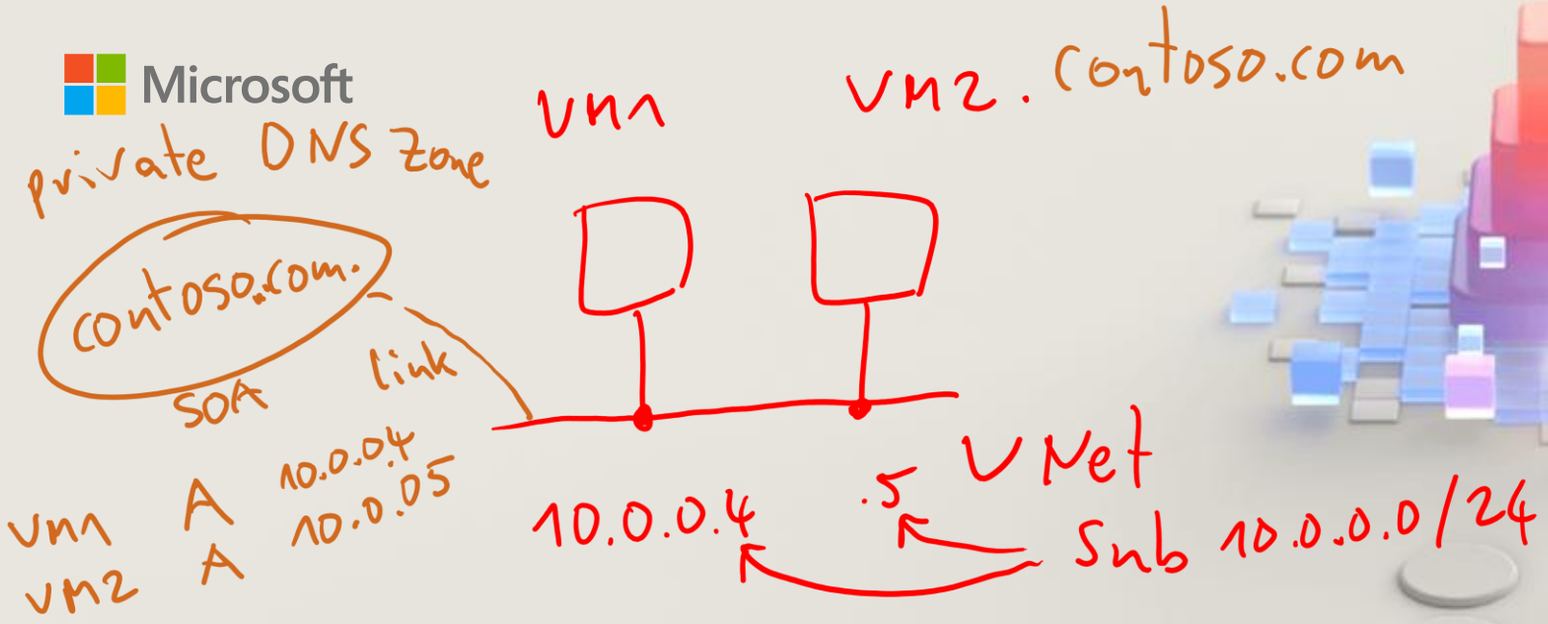
MODULE

Manage and control traffic flow in your Azure deployment with routes

50 min

Azure • Solution Architect • Beginner

Microsoft



Create DNS zones and configure DNS settings

Agenda: Azure DNS

- What is Azure DNS?
- Instructor demonstration
  - How to create DNS records?
  - How to enable auto registration?
- Student exercise: Create DNS zones and configure DNS settings
- Review questions and reference module

What is Azure DNS?

Use your own custom domain names

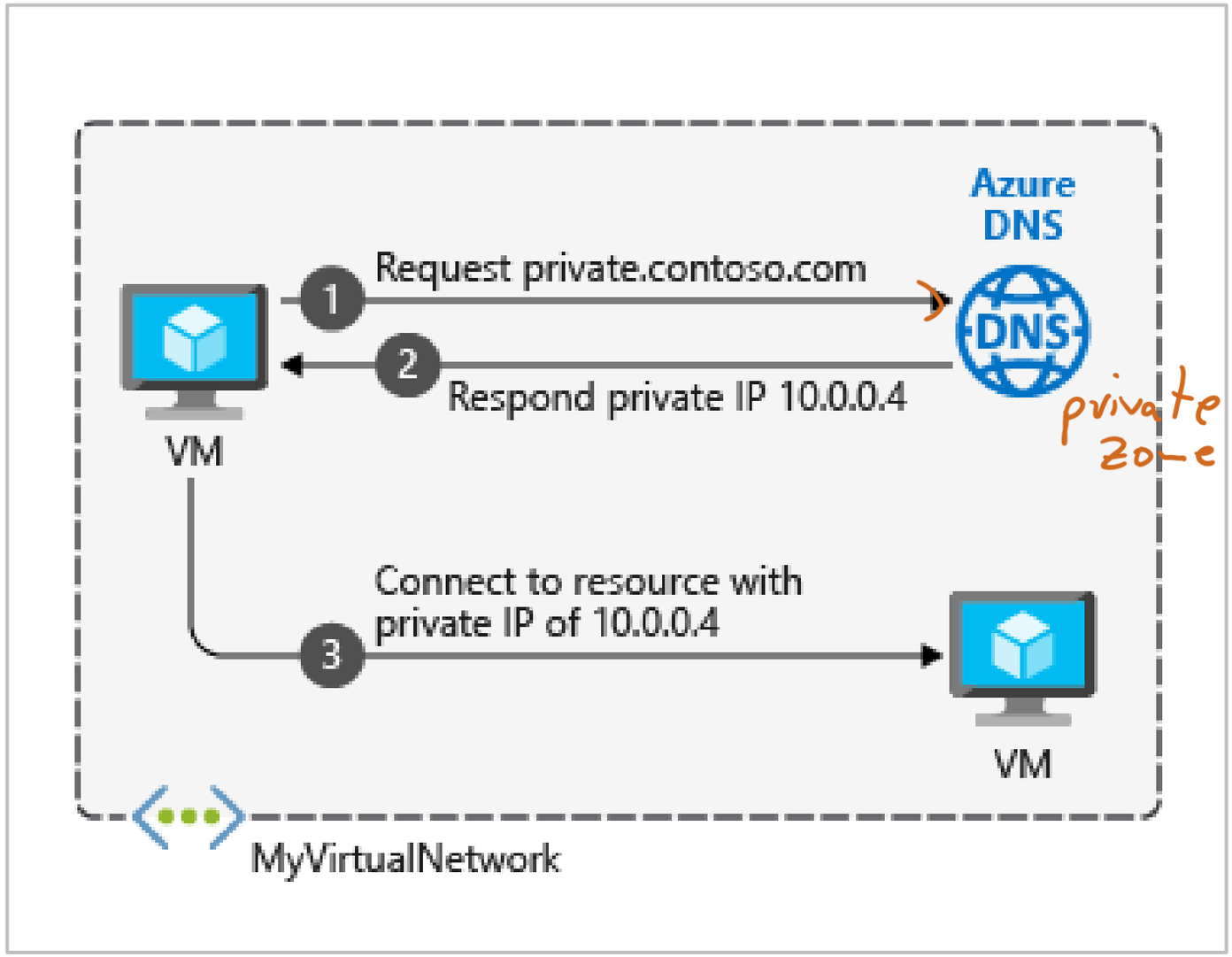
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

Removes the need for custom DNS solutions

Use all common DNS records types

Available in all Azure regions



Demo 05: DNS

- Create a private DNS Zone
- Add a DNS record set
- Link a VNet for auto registration

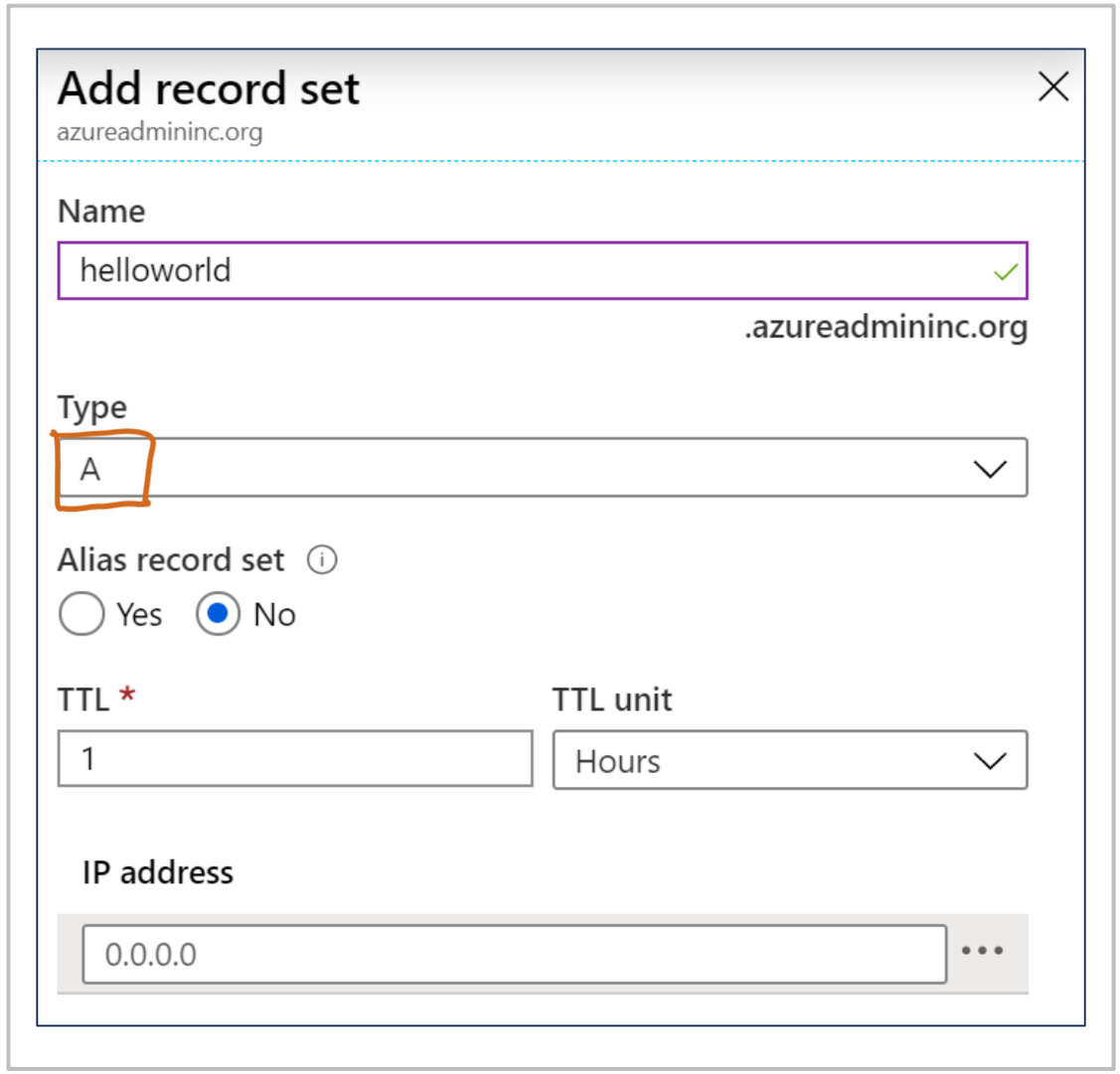
Add DNS Record Sets

A record set is a collection of records in a zone that have the same name and are the same type

You can add up to 20 records to any record set

A record set cannot contain two identical records

Changing the drop-down Type, changes the information required



Exercise 05: Create DNS zones and configure DNS settings

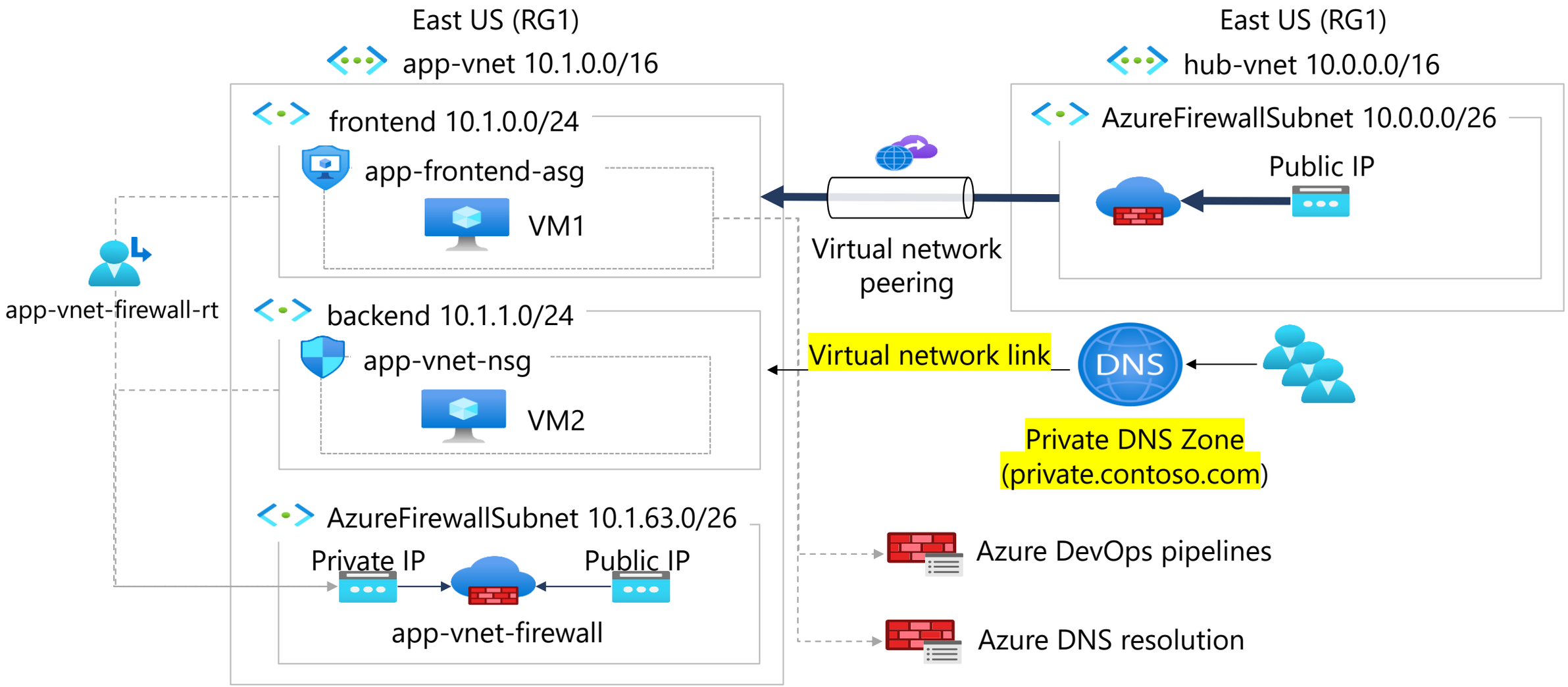
- Your organization requires workloads to use domain names instead of IP addresses for internal communications. The organization doesn't want to add a custom DNS solution.
- You identify these requirements.
  - A private DNS zone is required for contoso.com.
  - The DNS will use a virtual network link from app-vnet.
  - A new DNS record is required for the backend subnet.

Skilling tasks:

- ❑ Create and configure a private DNS zone.
- ❑ Create and configure DNS records.
- ❑ Configure DNS settings on a virtual network.

Architecture diagram

Exercise 05: Architecture diagram



Review and reference – Azure DNS

Check your knowledge questions and additional study

What is the main purpose of Azure DNS?

What does Azure Private DNS support?

MODULE

Host your domain on Azure DNS

43 min

Azure • Administrator • Beginner

Exercise 01: Create and configure virtual networks

Your organization is migrating a web-based application to Azure. Your first task is to put in place the virtual networks and subnets. You also need to securely peer the virtual networks.

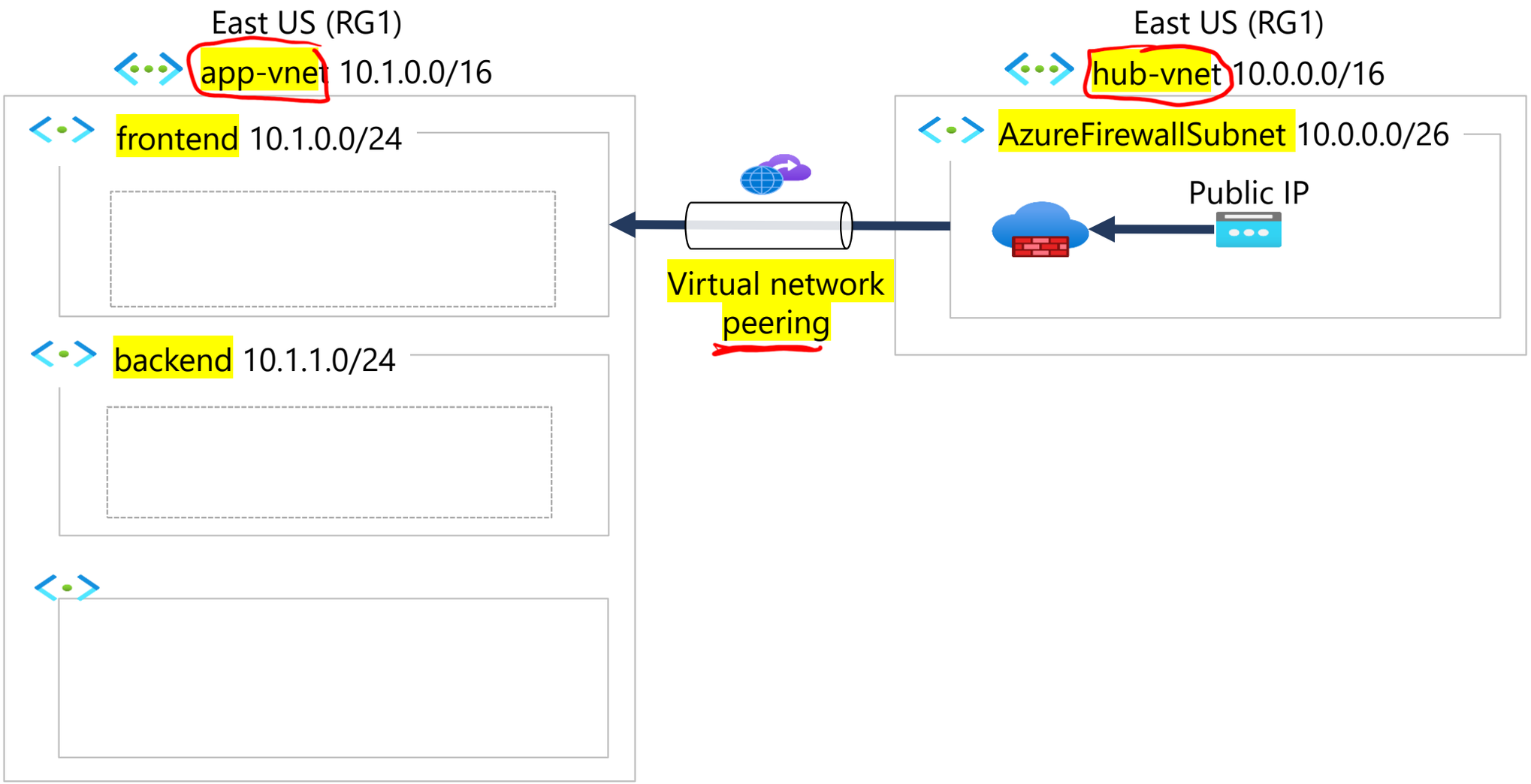
- Two virtual networks are required, app-vnet and hub-vnet.
- The app-vnet will host the application. This virtual network requires two subnets. The frontend subnet will host the web servers. The backend subnet will host the database servers.
- The hub-vnet only requires a subnet for the firewall.
- The two virtual networks must be able to communicate with each other securely
- Both virtual networks should be in the same region.

Skilling tasks:

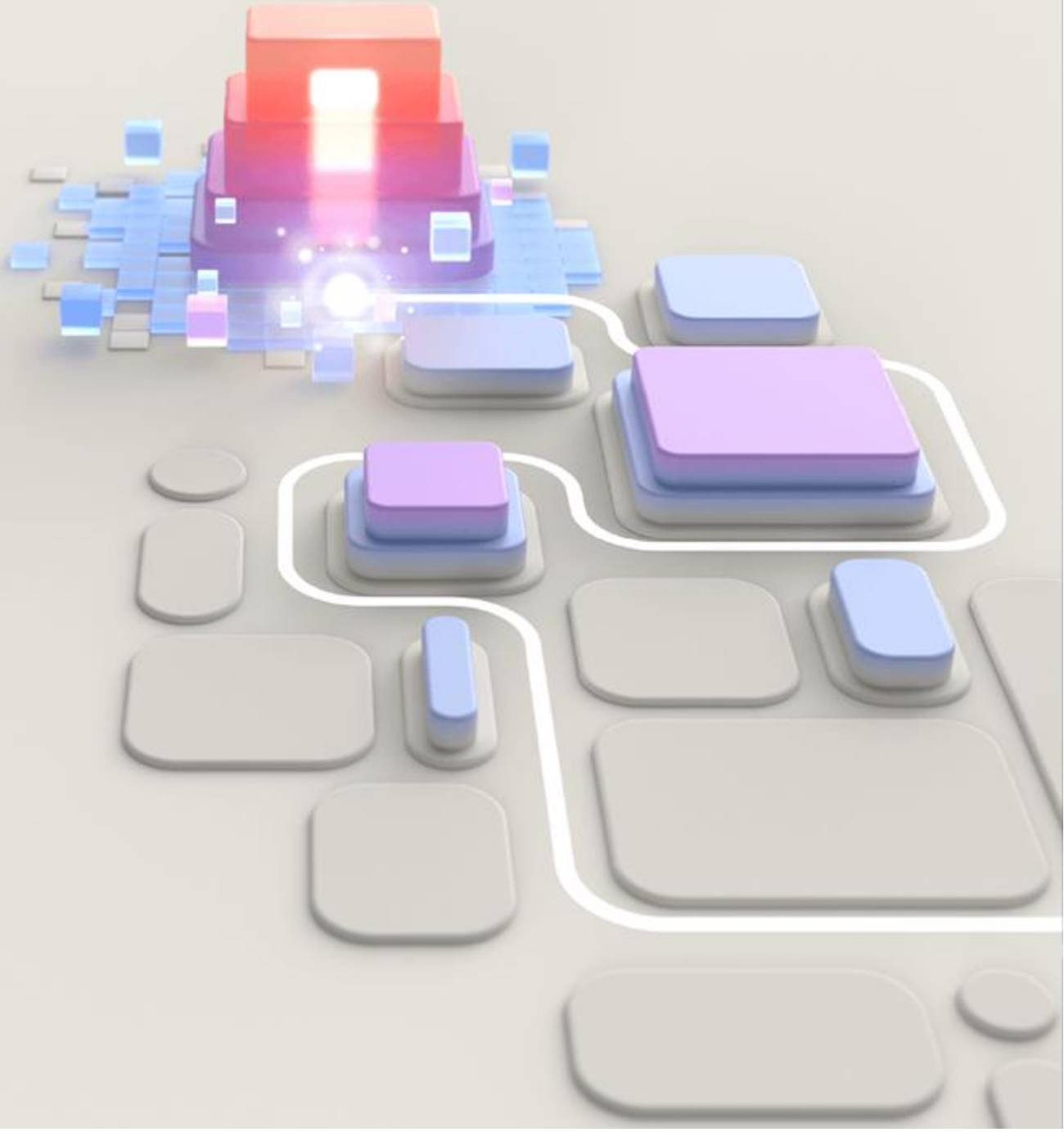
- ❑ Navigating the portal
- ❑ Create a virtual network
- ❑ Configure subnets
- ❑ Configure virtual network peering

Architecture diagram

Exercise 01: Create and configure virtual networks



Microsoft



End of presentation