CONFIGURE SECURE ACCESS TO YOUR WORKLOADS USING AZURE VIRTUAL NETWORKING

Course Code: 834014

This course is designed for students who are planning to Configure Secure Access to your Workloads using Azure Virtual Networking.

In this learning path, you practice configuring secure access to workloads using Azure networking.

What You'll Learn

Students will learn to,

- Configure virtual networks
- Configure Azure Virtual Network peering
- Manage and control traffic flow in your Azure deployment with routes
- Host your domain on Azure DNS
- Configure network security groups
- Introduction to Azure Firewall
- Guided Project - Configure secure access to workloads with Azure virtual networking services

Who Needs to Attend

Students who are performing Azure Administrator network security tasks in their day-to-day job, Network Engineers.

CONFIGURE SECURE ACCESS TO YOUR WORKLOADS USING AZURE VIRTUAL NETWORKING

Course Code: 834014

CLASSROOM LIVE	$675 CAD	1 Day

Classroom Live Outline

Module 1: Configure virtual networks

- Describe Azure virtual network features and components.
- Identify features and usage cases for subnets and subnetting.
- Identify usage cases for private and public IP addresses.
- Create a virtual network and assign IP address.

Module 2: Configure Azure Virtual Network peering

- Identify usage cases and product features of Azure Virtual Network peering.
- Configure your network to implement Azure VPN Gateway for transit connectivity.
- Extend peering by using a hub and spoke network with user-defined routes and service chaining.

Module 3: Manage and control traffic flow in your Azure deployment with routes

- Identify the routing capabilities of an Azure virtual network
- Configure routing within a virtual network
- Deploy a basic network virtual appliance
- Configure routing to send traffic through a network virtual appliance

Module 4: Host your domain on Azure DNS

- Configure Azure DNS to host your domain.

Module 5: Configure network security groups

- Determine when to use network security groups.
- Create network security groups.
- Implement and evaluate network security group rules.
- Describe the function of application security groups.

Module 6: Introduction to Azure Firewall

- Explain how Azure Firewall and Azure Firewall Manager work together to

protect Azure virtual networks.
- Evaluate whether Azure Firewall is the right solution to protect your Azure virtual networks from malicious incoming and outgoing traffic.
- Evaluate whether Azure Firewall Premium is the right solution to protect your Azure virtual networks from malicious incoming and outgoing traffic.
- Evaluate whether Azure Firewall Manager is the right solution for deploying policies across multiple firewalls.
- Identify and describe use cases for Azure Firewall and Azure Firewall Manager.

Module 7: Guided Project - Configure secure access to workloads with Azure virtual networking services
- Create and configure virtual networks
- Create and configure network security groups (NSGs)
- Create and configure Azure Firewall
- Configure network routing
- Create DNS zones and configure DNS settings

CONFIGURE SECURE ACCESS TO YOUR WORKLOADS USING AZURE VIRTUAL NETWORKING

Course Code: 834014

VIRTUAL CLASSROOM LIVE	$675 CAD	1 Day

Virtual Classroom Live Outline

Module 1: Configure virtual networks

- Describe Azure virtual network features and components.
- Identify features and usage cases for subnets and subnetting.
- Identify usage cases for private and public IP addresses.
- Create a virtual network and assign IP address.

Module 2: Configure Azure Virtual Network peering

- Identify usage cases and product features of Azure Virtual Network peering.
- Configure your network to implement Azure VPN Gateway for transit connectivity.
- Extend peering by using a hub and spoke network with user-defined routes and service chaining.

Module 3: Manage and control traffic flow in your Azure deployment with routes

- Identify the routing capabilities of an Azure virtual network
- Configure routing within a virtual network
- Deploy a basic network virtual appliance
- Configure routing to send traffic through a network virtual appliance

Module 4: Host your domain on Azure DNS

- Configure Azure DNS to host your domain.

Module 5: Configure network security groups

- Determine when to use network security groups.
- Create network security groups.
- Implement and evaluate network security group rules.
- Describe the function of application security groups.

Module 6: Introduction to Azure Firewall

- Explain how Azure Firewall and Azure Firewall Manager work together to

protect Azure virtual networks.
- Evaluate whether Azure Firewall is the right solution to protect your Azure virtual networks from malicious incoming and outgoing traffic.
- Evaluate whether Azure Firewall Premium is the right solution to protect your Azure virtual networks from malicious incoming and outgoing traffic.
- Evaluate whether Azure Firewall Manager is the right solution for deploying policies across multiple firewalls.
- Identify and describe use cases for Azure Firewall and Azure Firewall Manager.

Module 7: Guided Project - Configure secure access to workloads with Azure virtual networking services
- Create and configure virtual networks
- Create and configure network security groups (NSGs)
- Create and configure Azure Firewall
- Configure network routing
- Create DNS zones and configure DNS settings

Jul 6 - 6, 2026 | 9:00 AM - 5:00 PM EDT

Oct 5 - 5, 2026 | 9:00 AM - 5:00 PM EDT

CONFIGURE SECURE ACCESS TO YOUR WORKLOADS USING AZURE VIRTUAL NETWORKING

Course Code: 834014

PRIVATE GROUP TRAINING	1 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.