Cyber Shujaa

Cloud Security Specialist

Assignment 10: AZ-500 Learning Path - Secure Networking

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

In this assignment, we will learn the knowledge and skills needed to plan and implement robust security measures for Azure virtual networks, ensuring the confidentiality, integrity, and availability of network resources.

Microsoft Cloud Security Benchmark: Data Protection, Logging and Threat Detection, and Network Security

The goal of the topic related to Microsoft security benchmarks, specifically concerning data protection, logging, threat detection, and network security, is to provide organizations with guidelines and best practices to enhance their security posture.

This includes ensuring the confidentiality, integrity, and availability of data and resources, effectively monitoring and logging security events, detecting potential threats, and implementing robust network security measures to protect against cyberattacks.

By following these benchmarks, organizations can better safeguard their assets and maintain compliance with security standards such as NIST, CIS, and PCI-DSS.

What is an Azure Virtual Network

Azure Virtual Network is a fundamental component of Azure that allows users to create private networks in the cloud. It provides a secure and isolated environment for Azure resources to communicate with each other, as well as with on-premises networks and the internet. Key features of Azure Virtual Network include:

- Isolation: Each virtual network is isolated from others, ensuring that network traffic is not accessible to other Azure customers.
- Connectivity: It supports various connectivity options, including VPN gateways for secure remote access and Virtual Network peering for connecting multiple virtual networks.
- Security: Users can implement security measures such as Network Security Groups (NSGs) to control inbound and outbound traffic, enhancing the security of their applications and data.
- Routing: Azure Virtual Network allows for user-defined routes (UDRs) to optimize network traffic routing, ensuring efficient data flow between resources.

Azure Virtual Network Manager

Azure Virtual Network Manager is a management service that enables you to group, configure, deploy, and manage virtual networks globally across subscriptions. With Virtual Network Manager, you can define network groups to identify and logically segment your virtual networks. Then you can determine the connectivity and security configurations you want and apply them across all the selected virtual networks in network groups at once.

Network Security Groups (NSGs) and Application Security Groups (ASGs)

NSGs are crucial for controlling inbound and outbound traffic to Azure resources, while ASGs allow you to group resources based on their application needs.

We use NSGs to create specific rules that dictate which IP addresses, ports, and protocols are allowed or denied. For ASGs, we categorize our resources based on their application roles, which simplifies management and rule application.

User-Defined Routes (UDRs)

UDRs allow you to control the routing of network traffic by defining specific routes for packets to follow.
Implementing UDRs involves a systematic approach. First, we need to create the UDRs in the Azure portal or using Azure PowerShell or CLI. Specify the address prefixes for the destination and the next hop type, which can include options like Virtual Appliance or Internet. After creating the UDRs, associate them with the relevant subnets.

Virtual Network peering or gateway

Virtual network peering connects two Azure virtual networks. Once peered, the virtual networks appear as one for connectivity purposes. Traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, through private IP addresses only. No public internet is involved. You can also peer virtual networks across Azure regions (global peering).

A VPN gateway is a specific type of virtual network gateway that is used to send traffic between an Azure virtual network and an on-premises location over the public internet. You can also use a VPN gateway to send traffic between Azure virtual networks. Each virtual network can have at most one VPN gateway. You should enable Azure Distributed Denial of Service (DDoS) Protection Standard on any perimeter virtual network.

Gateway transit enables you to use a peered virtual network's gateway for connecting to on-premises, instead of creating a new gateway for connectivity. Gateway transit allows you to share an ExpressRoute or VPN gateway with all peered virtual networks and lets you manage the connectivity in one place.

Virtual Wide Area Network, including a secured virtual hub

A Virtual WAN connects to your resources in Azure over an IPsec/IKE (IKEv1 and IKEv2) VPN connection. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.

A hub is a virtual network that can contain gateways for site-to-site, ExpressRoute, or point-to-site functionality.

Secure VPN connectivity, including point-to-site and site-to-site

A Site-to-Site (S2S) VPN gateway connection is a connection over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. S2S connections can be used for cross-premises and hybrid configurations. A S2S connection requires a VPN device located on-premises that has a public IP address assigned to it.

A point-to-site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.

Connecting a virtual network to another virtual network (VNet-to-VNet) is similar to connecting a VNet to an on-premises site location. Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE. You can even combine VNet-to-VNet communication with multi-site connection configurations.

Azure Virtual Network encryption

Azure Virtual Network encryption is a feature of Azure Virtual Networks. Virtual network encryption allows you to seamlessly encrypt and decrypt traffic between Azure Virtual Machines by creating a Datagram Transport Layer Security (DTLS) tunnel.

Azure ExpressRoute

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

ExpressRoute connections offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet, because they don’t go over the public Internet.

Monitor network security by using Network Watcher

Azure Network Watcher provides a suite of tools to monitor, diagnose, view metrics, and enable or disable logs for Azure IaaS (Infrastructure-as-a-Service) resources. Network Watcher enables you to monitor and repair the network health of IaaS products like virtual machines (VMs), virtual networks (VNets), application gateways, load balancers, etc. Network Watcher isn't designed or intended for PaaS monitoring or Web analytics.
Network Watcher consists of three major sets of tools and capabilities:

- Monitoring
- Network diagnostic tools
- Traffic

Conclusion

To conclude, we have learned how to plan and implement comprehensive security measures for Azure virtual networks, including the use of Network Security Groups (NSGs), Application Security Groups (ASGs), user-defined routes (UDRs), Virtual Network peering, VPN gateways, Virtual WAN, VPN connectivity, ExpressRoute encryption, firewall settings for PaaS resources, and network security monitoring with Network Watcher.
https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/VJT9J4GM?sharingId=1C66F93EC0530812