Cyber Shujaa

Cloud Security Specialist

Assignment 12: AZ-500 Learning Path - Secure Networking

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

This assignment will teach us the knowledge and expertise necessary to design, implement, and manage a comprehensive security strategy for public access to Azure resources. We will be able to secure web applications, APIs, and network traffic effectively, ensuring the availability and performance of critical services while protecting against security threats.

Plan and implement Transport Layer Security (TLS) to applications, including Azure App Service and API Management

Azure provides encryption capabilities for data at rest in storage solutions, including file, disk, blob, and table storage. Microsoft also provides encryption to protect Azure SQL Database, Azure Cosmos DB, and Azure Data Lake.
Examples of these encryption services are;

- Azure disk encryption
- Azure Storage Service Encryption

For SQL Databases, Azure provides;

- Transparent Data Encryption
- Always Encrypted feature
- Cell-level or column-level encryption

Cosmos DB has;

- Azure Cosmos DB database encryption
  User data stored in Azure Cosmos DB in non-volatile storage (solid-state drives) is encrypted by default. There are no controls to turn it on or off.

At-rest encryption in Data Lake
Three types of keys are used in encrypting and decrypting data:

- Master Encryption Key (MEK),
- Data Encryption Key (DEK),
- Block Encryption Key (BEK).

For data in transit, Azure offers many mechanisms for keeping data private as it moves from one location to another.

- Data-link Layer encryption in Azure
- TLS encryption in Azure

Plan, implement, and manage an Azure Firewall, Azure Firewall Manager, and firewall policies

Azure Firewall is a cloud-native and intelligent network firewall security service that provides the best-of-breed threat protection for your cloud workloads running in Azure.

- **Azure Firewall Standard** provides layer 3 to layer 7 (L3-L7) filtering and threat intelligence feeds directly from Microsoft Cyber Security. Threat intelligence-based filtering can alert and deny traffic from/to known malicious IP addresses and domains that are updated in real time to protect against new and emerging attacks.
- **Azure Firewall Premium** provides advanced capabilities, including a signature-based intrusion detection and prevention system (IDPS) to allow rapid detection of attacks by looking for specific patterns.
- **Azure Firewall Basic** is intended for small and medium-sized (SMB) customers to secure their Azure cloud environments

Azure Firewall Manager simplifies the management of multiple firewalls and policies, allowing for centralized control. Firewall Manager can provide security management for two network architecture types:

- Secured virtual hub

An Azure Virtual WAN Hub is a Microsoft-managed resource that lets you easily create hub and spoke architectures.

- Hub virtual network

This is a standard Azure virtual network that you create and manage yourself.

Plan and implement an Azure Application Gateway

Azure Application Gateway is a web traffic (OSI layer 7) load balancer that enables you to manage traffic to your web applications.

An application gateway serves as the single point of contact for clients. It distributes incoming application traffic across multiple backend pools, which include Azure VMs, virtual machine scale sets, Azure App Service, and on-premises/external servers.

Plan and implement a Web Application Firewall (WAF)

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities.WAF can be deployed with Azure Application Gateway, Azure Front Door, and Azure Content Delivery Network (CDN) service from Microsoft.

Plan and implement an Azure Front Door, including Content Delivery Network (CDN)

Azure Front Door is Microsoft’s modern cloud Content Delivery Network (CDN) that provides fast, reliable, and secure access between your users and your applications’ static and dynamic web content across the globe.

Recommend when to use Azure DDoS Protection Standard

Azure DDoS Protection, combined with application design best practices, provides enhanced DDoS mitigation features to defend against DDoS attacks.

Azure DDoS Protection protects at the layer 3 and layer 4 network layers. For web application protection at layer 7, you need to add protection at the application layer using a WAF offering.

- DDoS Network Protection

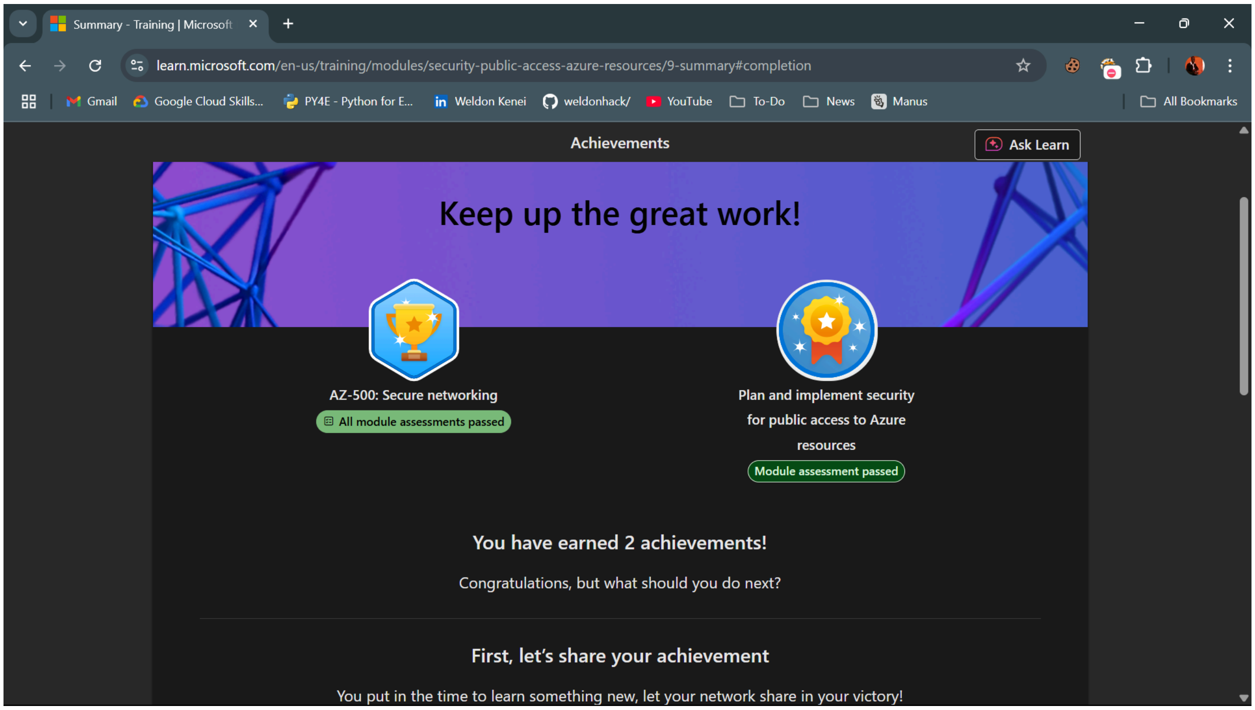
It's automatically tuned to help protect your specific Azure resources in a virtual network.

- DDoS IP Protection

DDoS IP Protection is a pay-per-protected IP model.

Conclusion

In this module, we learned how to plan and implement robust security measures for public access to Azure resources, including the use of Transport Layer Security (TLS) for applications, deploying and managing Azure Firewall with Azure Firewall Manager and firewall policies, configuring Azure Application Gateway and Azure Front Door with Content Delivery Network (CDN) for improved application performance and security, setting up a Web Application Firewall (WAF) for protection against web-based attacks, and making informed recommendations on when to use Azure DDoS Protection Standard to defend against distributed denial-of-service (DDoS) attacks.
https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/H7Z9UPL8?sharingId=1C66F93EC0530812


Summary - Training | Microsoft
learn.microsoft.com/en-us/training/modules/security-public-access-azure-resources/9-summary#completion
Gmail
Google Cloud Skills...
PY4E - Python for E...
Weldon Kenei
weldonhack/
YouTube
To-Do
News
Manus
All Bookmarks
Ask Learn

Achievements

Keep up the great work!

AZ-500: Secure networking

All module assessments passed

Plan and implement security for public access to Azure resources

Module assessment passed

You have earned 2 achievements!

Congratulations, but what should you do next?

First, let's share your achievement

You put in the time to learn something new, let your network share in your victory!