Microsoft ADC Cybersecurity Skilling Program

Week 7 Assignment

Student Name: Vincent Onchieku Collins

Student ID: ADC-CSS02-25052

Introduction

This week I worked through the AZ-500 Learning Path: Secure Networking, which is part of the Microsoft Certified: Azure Security Engineer Associate certification. The focus was on the first module:

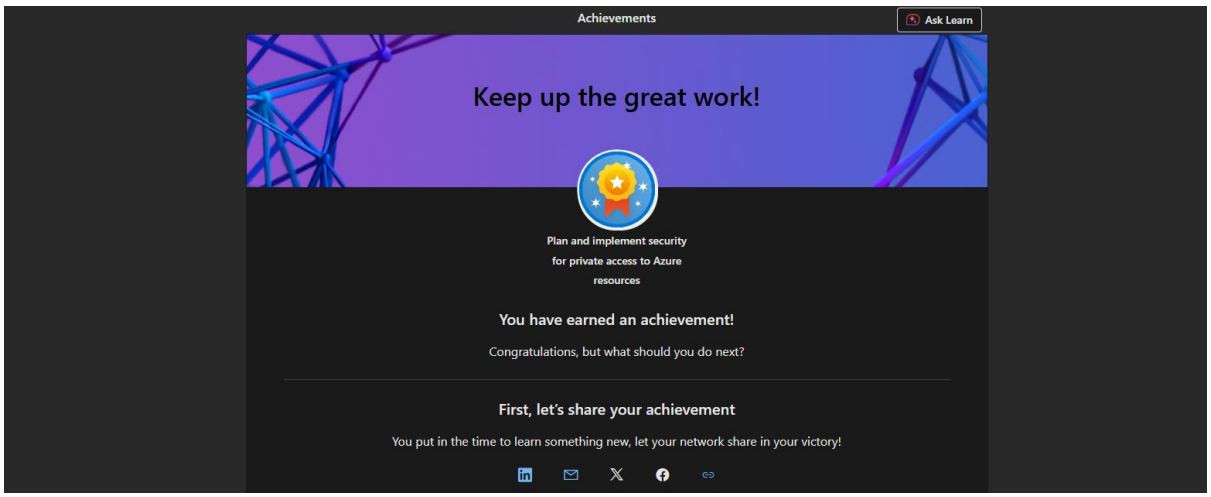
1. Plan and implement security for private access to Azure resources.
2. Plan and implement security for public access to Azure resources.

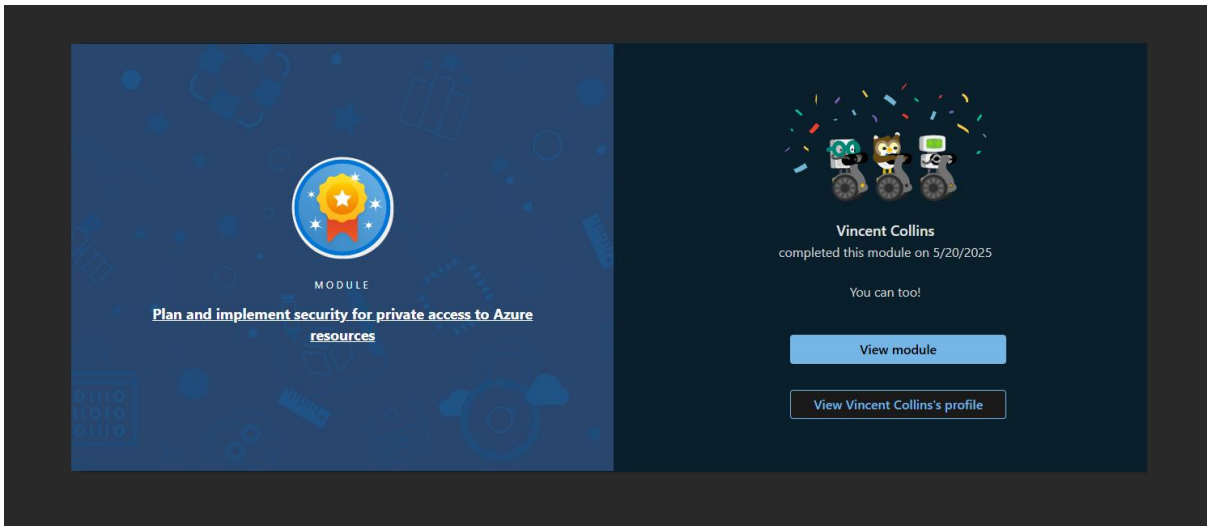
Tasks Completed

1. Plan and implement security for private access to Azure resources.

This module covers the design and deployment of secure, private network access strategies within Microsoft Azure. It focuses on protecting sensitive data by ensuring that resources like databases, applications, and services are only accessible through trusted internal networks. Key areas include the implementation of Virtual Network Service Endpoints and Private Endpoints, the use of Private Link services to expose services securely, and integrating services such as Azure App Service and Azure Functions into virtual networks for isolation. Participants also learn how to configure App Service Environments (ASEs) and secure Azure SQL Managed Instances, ensuring tight control over access and data flow within the Azure environment.

Verification link: https://learn.microsoft.com/en-us/users/vincentcollins-8814/achievements/juhdkmct

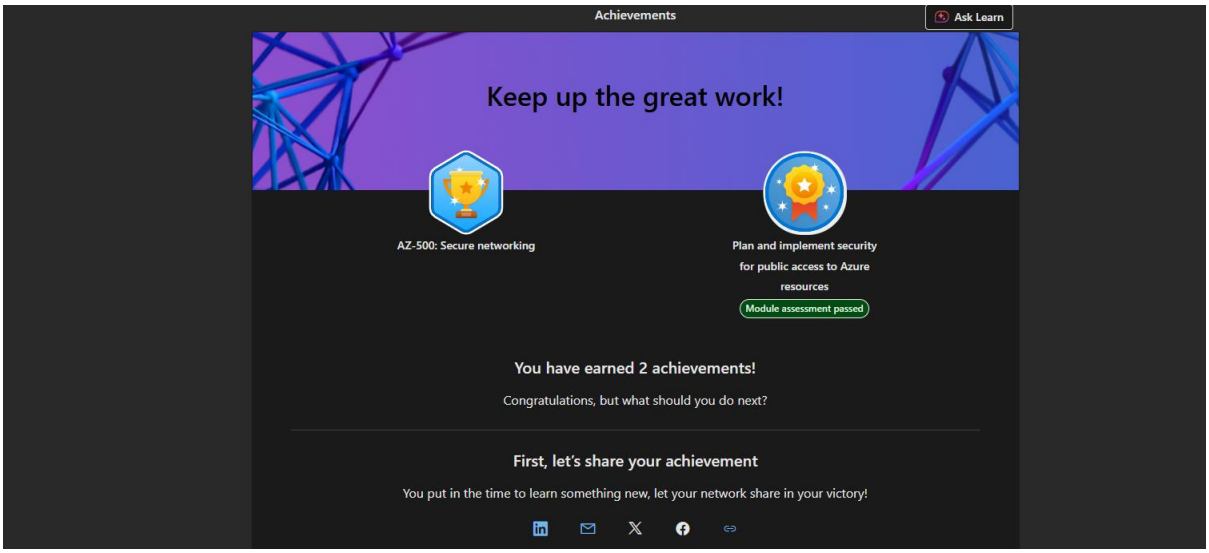

Achievements
Ask Learn
Keep up the great work!
Plan and implement security for private access to Azure resources
You have earned an achievement!
Congratulations, but what should you do next?
First, let's share your achievement
You put in the time to learn something new, let your network share in your victory!

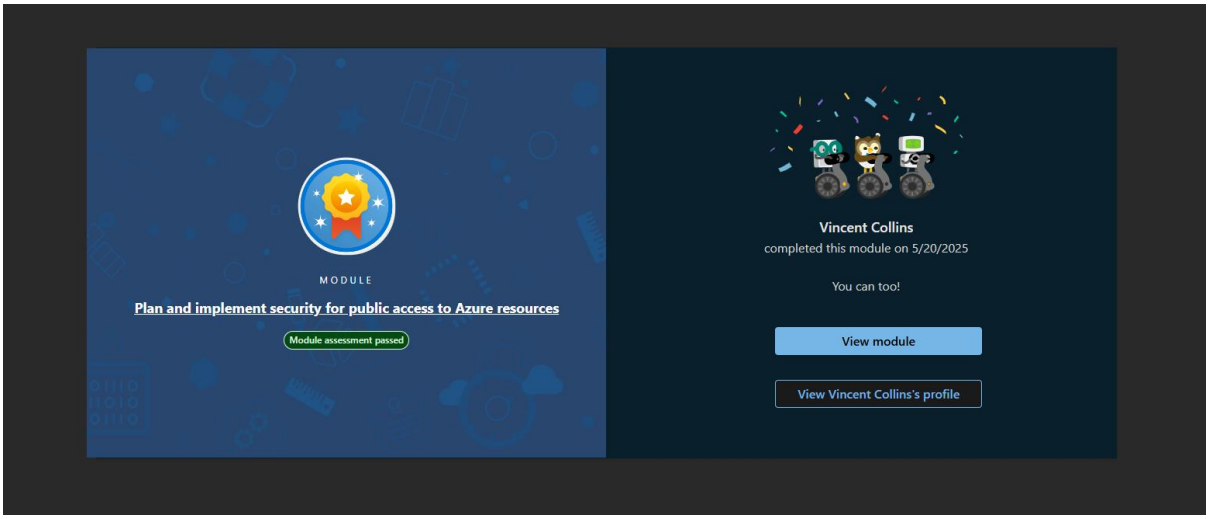

MODULE
Plan and implement security for private access to Azure resources
Vincent Collins
completed this module on 5/20/2025
You can too!
View module
View Vincent Collins's profile

2. Plan and implement security for public access to Azure resources.

This module equips administrators with the tools and knowledge needed to protect Azure-hosted applications and services that are publicly accessible. The focus is on maintaining confidentiality, integrity, and availability by implementing technologies like Transport Layer Security (TLS), Azure Firewall and Firewall Manager, and application-level protections through Azure Application Gateway and Azure Front Door with integrated Content Delivery Network (CDN). The module also dives into Web Application Firewall (WAF) configuration to guard against common web vulnerabilities, and guidance on when to use Azure DDoS Protection Standard to mitigate distributed denial-of-service threats. Together, these skills ensure secure and optimized public access to critical Azure-hosted resources.

verification link: https://learn.microsoft.com/en-us/users/vincentcollins-8814/achievements/9yac6p7u





Conclusion

The two AZ-500 modules provide a comprehensive understanding of how to secure Azure environments from both internal and external threats. By learning to implement private access strategies using tools like Private Endpoints, Virtual Network Service Endpoints, and Private Link, professionals can ensure sensitive resources remain isolated and accessible only through secure channels. On the other hand, mastering public access security techniques such as configuring TLS, Azure Firewall, Application Gateway, Front Door, WAF, and DDoS Protection enables secure, scalable, and resilient access to web applications and APIs exposed to the internet.

These modules emphasize a defense-in-depth approach, ensuring that administrators are well-equipped to design and enforce layered security measures that protect Azure resources, regardless of how they are accessed. The combined knowledge strengthens your ability to architect secure Azure solutions that balance performance, usability, and robust security critical for supporting enterprise-grade applications in the cloud.