Enterprise Network Architecture - Short Paper

Objective

Network architecture diagrams provide a visualization of the current network structure of an organization. They are a great way to view logical placement of security controls and identify security gaps in the network. For this paper, you will design a secure network architecture for the use case defined in the requirements section below.

Requirements

"Connected Networks" is a small *hosting service provider* that hosts eCommerce websites for its clients.

"Farm-vacations" is a travel company that provides its customers farm vacation rentals. They do not own a data center and need to host their customer-facing website and supporting services on Connected Networks hosting service.

As a Solutions Architect of Connected Networks, **you** will design a logical network diagram for hosting Farm-vacations systems.

Below are the requirements.

1. **Customer Facing Service**

   The customer-facing website lets vacationers browse, search, and book trips. The current website is an asp.net application that runs on IIS over TLS (https) and SQL Server 2016. Traffic volume to this website is low, but the website should be reliable to process every booking request.

   a. Design a network to host the web application server. Add appropriate network segments (tiers) to separate customer facing (internet) systems from the backend database systems.
   b. Deploy firewall to restrict only specific traffic between the external facing and internal networks.

2. **Service Provider Administration**

   As part of their hosting services, Connected Network's internal staff provides support and maintenance for the Farm-Vacations' website. Connected Network also provides its customers security as part of the hosted service. This includes network monitoring for

intrusion attempts and web application firewall. All system logs are sent to an isolated monitoring network.

a. Update the network diagram to show how connected network's internal staff provides support and maintenance to this website.
b. Add other security devices in your logical diagram to provide the intrusion detection and protection services.

3. Service Customer Administration

The client Farm-vacations would like to create an inventory management portal that must be accessible to their internal staff from their office network **only (**not to be accessed from anywhere on the internet). This portal will be used to create new listings, remove old ones and update listing details.

a. Add a business to business (B2B) VPN connection to allow Farm-vacations staff to access the inventory portal.

Additional Details

1. The Network Engineer at Connected Networks is responsible to provide IP Address allocation. You have them to provide you IP addresses for the Farm Vacation internal systems and the public IP for the website.
    a. The Network Engineer has provided you with following netblock for the Farm-Vacations project - **10.24.10.0/24**
    b. Public IP reserved for their rental website - 54.168.122.129
    c. A DNS entry on Connected Network's DNS server for the domain name "www.farmvacations.com" pointing to the Public IP Address 54.168.122.129 has been added.
    d. The B2B VPN is configured for Farm Vacations. Network IP address allocated to Farm Vacations source system on the VPN Interface - 10.54.90.0/24
2. You checked with the Application Engineer and they have provided the following details about the application specifications / configurations -
    a. Both customer facing app and inventory management portal are accessible on https over port 443
    b. The application server communicates with the database server over port 1433
    c. The administration of the web server is done using RDP on port 3389
3. You have requested the Internal Connected Networks Security team (who manages firewall and other security devices) to provide you will their administration network details. You need this information to add to your logical network diagram for Farm Vacations network.
    a. They will need port 22 (ssh) access from the administration subnet to the firewall.
    b. Syslog services use UDP port 514 to send logs from servers to Log Management server
    c. The Connected Networks' internal administration subnet is on 10.10.10.0/24 network segment.

Report

Submit a pdf document with 4-6 pages containing the following.

1. Part I
    a. For the requirements specified in the “Requirements Section”, create a network architecture diagram.
    b. Provide a brief description of the network architecture you created.
    c. Include description of systems and network components on your network.
    d. Include details on the network subnets (segments) and why did you create the network segments. What IP addressing schemes you used.
    e. Firewall rules and policies to allow and deny traffic between each segment. Ensure your rules include source network, destination network, ports/protocols.
2. Part II
    a. What security controls you implemented in the network architecture and why?
    b. Do you see any threats to your network architecture? if yes, explain what and possible solutions to mitigate them briefly.

Note: If the requirements are lacking on specific information, you can make assumptions to complete your network diagram. if you make any assumptions in your work, ensure you specify it in your report.

References

The link provides high level details on network architecture and security controls.

Both AWS and Azure provide reference architecture diagrams, these can be referenced to create a tiered network.

If you are using Visio, download and install Microsoft Visio from CCIS MSDNAA site. Note you will need a CCIS account for signing up for a MSDNAA account. The MSDNAA account credentials will be sent to your email ID and this process takes up to 2-3 days so plan accordingly. You can sign-up for MSDNAA account here.