Exercise: Firewall design and configuration

Introduction

You've learned about Azure Firewall and its role in securing virtual networks in Microsoft Azure. Now, it's time to put your knowledge into practice by designing an Azure Firewall for a fictional company called ABC Inc.

Case study

ABC Inc. is a software development company that specializes in cloud-based applications. It has multiple Azure virtual networks set up to manage its development, testing, and production environments. The company wants to implement a centralized firewall to control traffic between these virtual networks and the internet. The company also wants to ensure that all traffic between its virtual networks is secure and follows specific rules to protect sensitive data.
Your task is to design an Azure Firewall solution for ABC Inc. that meets the requirements. Consider the following aspects while creating your design:

Step 1: Network topology selection

ABC Inc. has multiple Azure virtual networks that need to be connected to a centralized firewall for traffic control. Choose between two topology options: Hub-and-spoke topology or fully meshed topology. Provide a brief explanation for your chosen topology and its advantages for ABC Inc.'s requirements.

Hub-and-spoke topology

In this setup, you have a central hub virtual network where the Azure Firewall is deployed. The other virtual networks (spokes) are connected to the hub, and all traffic between spokes and the internet must go through the hub.

Fully meshed topology

In this setup, all virtual networks are directly connected to each other and the Azure Firewall. Each virtual network can communicate with any other network without going through a central hub.

Step 2: Firewall rule identification

Identify and list the essential firewall rules that should be implemented to meet ABC Inc.'s requirements. These rules should allow and deny specific types of traffic to and from the virtual networks.

Step 3: Network Address Translation (NAT) rule assessment

Determine whether any NAT rules are necessary for the virtual networks to communicate with the internet.

Step 4: Application rule evaluation

Consider the need for application rules, which allow specific applications or services to be accessed from the virtual networks.

Step 5: Logging and monitoring setup

Explain the importance of enabling logging for Azure Firewall and how the company can monitor and analyze the logged data.

Step 6: High availability options

Discuss the options for making the Azure Firewall highly available to ensure continuous protection even during a failure.

Step 7: Security best practices

Highlight any security best practices that should be followed to secure the Azure Firewall and its associated resources effectively.

Conclusion

Prepare a written document that includes all the above aspects of your Azure Firewall design for ABC Inc. Use clear and concise language to explain your decisions and choices. You may use diagrams, bullet points, or any other appropriate format to present your ideas effectively.