Solution

Step 1: Network topology selection

Hub-and-spoke topology:

Hub-and-spoke topology would be the best option for ABC Inc. Hub can be used to deployed a central firewall through which all the traffic will pass before entering the virtual networks.

Advantages:

- Central firewall
- Monitor and control traffic
- Employ NSGs for extra layer of security

Step 2: Firewall rule identification

Network rules: ABC Inc. can implement network rules to allow or deny traffic between virtual networks based on IP addresses, ports and protocols.

Application rules: ABC Inc can configure application rules based on FQDNs. This can be used for external traffic FQDNs and deny rest of the traffic.

Step 3: Network Address Translation (NAT) rule assessment

ABCs would need to configure some NAT rules for its virtual network to communicate withe the internet. As ABC doesn't want to expose the ip of Virtual networks to internet, it would need to create a network address translation that would change the IP of virtual network to the Firewall Public IP address.

Step 4: Application rule evaluation

Implementing application rule is good practice that will help ABC Inc. to divide the network into different segments and it will also help in restricting the access to certain resources.

Step 5: Logging and monitoring setup

ABC can log and monitor traffic through NSGs and firewall. It will help the company to look out for suspicious activities. It can be achieved by observing various metrics provide by Azure firewall

Step 6: High availability options

Multiple availability zone provides redundancy and fault tolerance which is pre-built in Azure Firewall Premium.

Step 7: Security best practices

- Log and monitor firewalls
- Threat-based filtering
- Isolation of resources
- Network segmentation
- Use FQDN tags