Your organization hosts a VM that performs a security-related function. For both security and auditing purposes, you need to ensure that all traffic reaches the VM from a single IP address in another subnet, regardless of source. Which of the following solutions meets this requirement?

Step 1: Answer with Explanation

Answer: Use rules in Azure Firewall to route traffic to the target VM based on source and target IP addresses.

Explanation

For your cloud workloads operating in Azure, Azure Firewall is a cloud-native and intelligent network firewall security service that offers the greatest threat protection available. Fully stateful firewall as a service with unconstrained cloud scalability and built-in high availability.

The five pillars of excellent architecture form the foundation of Azure Firewall:

Reliability

Security

Cost reduction

excellence in operations

Using spreadsheets or firewall logs, you can keep an eye on Azure Firewall. Activity logs can also be used to audit actions performed on Azure Firewall resources.

Step 2: Explanation for incorrect option

An Azure Firewall monitors all traffic, but an NSG is more focused and deployed to certain subnets and/or network interfaces. Both firewall and NSG allow for the application of rules based on IP addresses, port numbers, networks, and subnets.

ASGs are used within an NSG to apply a network security rule to a particular workload or group of VMs. The network object, as described by the ASG, is added with explicit IP addresses.

You can designate network routes with User Defined Routing so that your Azure Virtual Appliances can manage traffic going both in and out of your subnets and to the Internet. IP forwarding needs to be enabled in order for the network interfaces to be permitted to accept and forward traffic.