Exam Session - Preview Exam: Designing and Implementing Microsoft Azure Networking Solutions (AZ-700)

cloudacademy.com/quiz/exam/3772191/results

#1

You have begun migrating your existing applications from on-premise servers to resources on an Azure Virtual Network. The on-premise network and Azure are currently connected via ExpressRoute. You need to ensure the ExpressRoute connection is healthy at all times. What Network Watcher service can you utilize to monitor the connection?

✓ Connection Monitor (formerly Network Performance Monitor)

✗ Traffic Analytics

✗ VPN Troubleshoot

✗ Connection Monitor (Classic)

Explanation

The new Connection Monitor (formerly the Network Performance Monitor service) is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.

Please note that Azure also has a legacy service that is also named Connection Monitor, but this has been changed to Connection Monitor Classic.

https://docs.microsoft.com/en-us/azure/azure-monitor/insights/network-performance-monitor?toc=%2fazure%2fnetwork-watcher%2ftoc.json

#2

You are troubleshooting a Network Security Group. Which of the following Azure PowerShell cmdlets will return all the rules applied to a Network Interface (NIC)?


Get-AzEffectiveNetworkSecurityGroup


Get-AzNsg


Get-AzNicNetworkSecurityGroup


Get-AzEffectiveNicNsg

Explanation

Use the following PowerShell cmdlet to return a list of all NSG rules applied to a network interface:

Get-AzEffectiveNetworkSecurityGroup -NetworkInterfaceName NIC1 -ResourceGroupName ResourceGroup1.


https://azure.microsoft.com/en-us/documentation/articles/virtual-network-nsg-troubleshoot-powershell/
#3

Because of the pandemic, you and your coworkers have been sent home. You all need to establish access between your home computers and the company's Azure Virtual Network. Which of the following will you need to do to configure this setup securely? Select 3.


Create a point-to-site VPN connection between your home computer and the Azure vNet


Generate and export a client certificate for your home computer


Install a VPN client on your home computer


Allowlist your home computer's IP address in the vNet's security group

Explanation

The best choice here would be to configure a Point to Site VPN connection. Since you do not need to make any changes to your company's network configuration, the client-side of the configuration only includes the following:

- Generate a client certificate for your computer
- Export the certificate
- Install and use a VPN client to configure site connection

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

#4

You have a two-tier application hosted within VNet-01 with an CIDR block of 10.0.0.0/16 and the following resource configurations:The front end is hosted on a VM named "VM_Front" within a public subnet. The public subnet has an IP address range of 10.0.2.0/24. VM_Front has a private IP address of 10.0.2.5, and a public IP address of 192.168.50.2.The backend is hosted on a second VM named VM_Back within a private subnet. The private subnet has an IP address range of 10.0.3.0/24. VM_Back has a private IP address of 10.0.3.4.A public load balancer with a private IP address of 10.0.1.6 and a public IP address of 172.16.50.35.You are configuring a final rule for a network security group (NSG) associated with resources in the private subnet where VM_Back is deployed. This final rule should block all traffic from the public subnet. Traffic from the public subnet that does not meet any of the NSG Allow rules would be processed by this rule.Which NSG rule parameters below would meet the requirements for this NSG rule?

```
Inbound Rule
Source: 10.0.2.0/24
Source Port: 0-65535
Destination: 10.0.3.4
Destination Port: 0-65535
Protocol: ANY
Priority: 4096
Action: Deny
```

```
Outbound Rule
Source: 10.0.2.0/24
Source Port: 0-65535
Destination: 10.0.3.4
Destination Port: 0-65535
Protocol: ANY
Priority: 20
Action: Deny
```

```
Inbound Rule
Source: 10.0.0.0/16
Source Port: *
Destination: 10.0.3.4
Destination Port: *
Protocol: ANY
Priority: 4096
Action: Deny
```

```
Outbound Rule
Source: 0.0.0.0/0
Source Port: *
Destination: 10.0.3.4
Destination Port: *
Protocol: ANY
Priority: 20
Action: Deny
```

Explanation

The correct NSG rule configuration is:

- Inbound Rule
- Source: 10.0.2.0/24
- Source Port: 0-65535
- Destination: 10.0.3.4
- Destination Port: 0-65535
- Protocol: ANY
- Priority: 4096
- Action: Deny

/course/implementing-azure-network-security/configuring-security-rules-in-an-nsg/#5

You deploy a new version of your company's website after the company has undergone an acquisition. Because of this, there is a new URL that reflects your parent company's new name. Your boss is concerned that older customers will still try to use the old URL. What's the best way to ensure old customers are redirected to the company's new URL?


Multi-site listeners


Basic routing


SSL termination


URL path-based routing

Explanation

URL path-based routing allows you to route traffic to the back-end server pools based on the URL paths of the request. Multi-site listening enables you to configure more than one web app on the same port, which is not applicable here. Basic routing only allows you to configure access/permissions for your network. SSL termination is for decrypting encrypted traffic before passing it to a web server.


https://docs.microsoft.com/en-us/azure/application-gateway/url-route-overview#:~:text=URL%20Path%20Based%20Routing%20allows,to%20different%20backend%20server%20pools.

#6

Your company has recently moved to a remote working environment. To protect the security of the private network hosting business-critical applications, you and your team have been instructed to use a VPN client to access the company network. Which tools would you use to monitor VPN connectivity should issues arrive? (Select 3).


Connection Monitor


Network Watcher

✗
Network Performance Monitor

✓
Traffic Analytics

Explanation

Any of these tools can be useful in monitoring VPN connectivity issues, particularly on a user level, except Network Performance Monitor. This service is being deprecated, and Network Performance Monitor tests should be migrated to Connection Monitor.

https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor-overview

#7

You would like to implement a Hub-and-Spoke VNet peering connection between two existing VNets in the East US region, (VNet 1 and VNet2), without using a network virtual appliance. You want resources in VNet1 and VNet2 to be able to communicate. You have deployed VNet3 in the East US region that will serve as a hub between the other VNets. VNet1 and VNet2 should be able to communicate with each other through VNet3 using a VPN virtual network gateway.Which VNet peering connections should be configured to allow all forwarded traffic?

✓
All peering connections between the hub and spokes

✗
No peering connections

✗
Only peering connections directed to VNet3 as the hub

✗
Only peering connections directed to VNet1 and VNet2 as the spokes

Explanation

Suppose you have several spokes that need to connect with each other. In that case, you'll run out of possible peering connections quickly, because the number of virtual network peerings per virtual network is limited. (For more information, see Networking limits. In this scenario,

consider using user-defined routes (UDRs) to force traffic destined to a spoke to be sent to Azure Firewall or a network virtual appliance acting as a router at the hub. This change will allow the spokes to connect to each other.

You can also configure spokes to use the hub gateway to communicate with remote networks. To allow gateway traffic to flow from spoke to hub and connect to remote networks, you must:

- Configure the peering connection in the hub to allow gateway transit.
- Configure the peering connection in each spoke to use remote gateways.
- Configure all peering connections to allow forwarded traffic.

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli

#8

Your IT consulting business has recently partnered with two other businesses in different regions of the country. Each of your three offices has resources deployed in Microsoft Azure cloud. Although you plan to eventually merge your separate offices into a single Azure AD tenant, you would like to connect several VNets in your separate subscriptions beforehand with your existing, separate Azure AD tenants in place.What Azure solution is the easiest way to accomplish this?

✓ Create VNet peering connection

✗ Create Virtual Network Gateways

✗ Create a DNS zone with split-horizon view

✗ Create a VNet-to-VNet VPN

Explanation

Microsoft Azure has steadily increased the compatibility of VNet Peering connections so that the previous generation solution, known as either Virtual Network Gateways or VPN Gateways, are used for in fewer scenarios now. VNet Peering connections can now connect VNets within separate subscriptions also within separate Azure AD tenants.

/course/azure-network-connectivity-name-resolution/virtual-network-gateways/

Covered in this lecture

Virtual Network Gateways

Course:Azure Network Connectivity and Name Resolution

5m

#9

You would like to implement a Hub-and-Spoke VNet peering connection between two existing VNets in the East US region, (VNet 1 and VNet2), without using a network virtual appliance. You want resources in VNet1 and VNet2 to be able to communicate. You have deployed VNet3 in the East US region that will serve as a hub between the other VNets. VNet1 and VNet2 should be able to communicate with each other through VNet3 using a VPN virtual network gateway.Which VNet peering connections should be configured to allow gateway transit?

✓ All peering connections between the hub and spokes

✗ No peering connections

✗ Only peering connections directed to VNet3 as the hub

✗ Only peering connections directed to VNet1 and VNet2 as the spokes

Explanation

Suppose you have several spokes that need to connect with each other. In that case, you'll run out of possible peering connections quickly, because the number of virtual network peerings per virtual network is limited. (For more information, see Networking limits. In this scenario, consider using user-defined routes (UDRs) to force traffic destined to a spoke to be sent to Azure Firewall or a network virtual appliance acting as a router at the hub. This change will allow the spokes to connect to each other.

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli

#10

Which of the following should you configure to ensure a virtual application located in East US (subnet VNetSub1) can communicate with a different application located in Central US (subnet VNetSub5)? Select the 2 that apply.


Virtual network peering


Global network peering


Security Groups


VPN Gateway

Explanation

To allow resources from two different subnets which are located in two separate Azure regions to communicate, you must configure Global network peering. Furthermore, you should edit each subnet's security groups to allow the appropriate inbound and outbound traffic to fully ensure appropriate access.

 https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

#11

You have an on-premises network that connects to VNet 1 through a VPN gateway connection. VNet 1 connects to VNet 2, VNet 3, and VNet 4, which are in the same region as VNet 1, via separate VNet peering connections. VNet 1 serves as a router between the on-premises network and VNets 2, 3, and 4. What do you call this kind of VNet architecture?


a Hub-and-spoke network


a VNet-to-VNet connection


a Global VNet Peering

a Site-to-Site VPN connections

Explanation

An alternative to peering all of the networks together is to use a hub-and-spoke topology, with the hub acting as a router. In this configuration, the only way for two spokes to communicate with each other is through the hub. One big advantage of this architecture is that you could put shared services in the hub that could be used by all of the spokes.

/course/azure-network-connectivity-name-resolution/virtual-network-peering/

Covered in this lecture

More Complex Scenarios

Course:Azure Network Connectivity and Name Resolution

2m

#12

There are four replicas of a multi-tier application separated into four resource groups with the following specifications: Each resource group is in a separate region - East US, West US, West Central US, and South Central US. Each resource group includes a replica of a three-tier application replica comprised of five VMs: Two front-end VMs, two mid-tier application VMs, and one back-end database VM. You would like to configure Azure network resources to accomplish the following: Route inbound requests to the application replica based on user location. Create a front-end firewall for all incoming requests from the internet Allow communication between resources in separate subnets while restricting the use of public IP addresses whenever possible. Encrypt all traffic throughout communication between different application layers. Load balance incoming requests from the public internet, as well as requests between each tier of the application. Monitor the performance of each VM in each application tier The senior solution architect on the project recommends implementing an Azure Traffic Manager, Azure Load Balancers, and Application Gateway. The senior architect describes how these Azure resources would manage incoming and outgoing traffic to meet the stated objectives. However, you suspect only some of his statements are correct, and others are incorrect. Looking at the statements below, which statements are correct? (Choose 2 answers)

Incoming requests would first reach an Azure Traffic Manager configured for geographic routing, which would deploy the requests to one of four application gateways.

Traffic would need to be approved by the application gateway before continuing to a public load balancer, which routes traffic to specific front-end VMs.

Traffic between resources without assigned public IP addresses would be load balanced by internal load balancers.

Outgoing response traffic from the front-end VMs would return through the traffic manager before it is sent to the external client.

Explanation

Geographic routing is similar to performance routing because it looks at the client's location. The difference is that you can specify exactly which region you want a client to connect to based on their location. For example, if your European customers require that their data stays in Europe, then you could always route them to a European region.

If you have an internal application that shouldn't be exposed to the internet, then don't assign a public IP address to the load balancer. Instead, it will use a private IP address. In this configuration, it's known as an internal load balancer.

 /course/designing-an-azure-network-implementation/azure-load-balancing/

#13

What should you do to configure gateway traffic to flow from spoke to hub and connect to remote networks?

Allow all peering connections between the hub and spokes

Allow no peering connections

Configure the peering connection in the hub to allow gateway transit, and then configure the peering connection in each spoke to use remote gateways.

Configure the peering connection in the hub to allow gateway transit, the peering connection in each spoke to use remote gateways, and configure all peering connections to allow forwarded traffic.

Explanation

You can configure spokes to use the hub gateway to communicate with remote networks. To allow gateway traffic to flow from spoke to hub and connect to remote networks, you must:

- Configure the peering connection in the hub to allow gateway transit.
- Configure the peering connection in each spoke to use remote gateways.
- Configure all peering connections to allow forwarded traffic.

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli

#14

You are an Azure Network Engineer that is designing the network configuration for hosting a three-tiered application. The application uses the following tiers in all daily business-critical operations: A SQL Database A JavaScript Frontend A processing middle tier The web application also interfaces with the following on-premise resources: A Windows File server A SQL server A Windows Domain Controller How many subnets would you recommend hosting the VMs for the web application?

✗
1

✓
3

✗
6

✗
2

Explanation

Because there are three web application layers, it would be preferential to have a separate subnet for each layer. The on-premise resources here are irrelevant as they are not part of the web application but rather just resources the web app must communicate with.

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/network-overview

#15

A company needs to connect their on-premise data center to Azure. They want to have a dedicated connection and at the same time want to have a failover connection. They don't mind having a drop in latency when it comes to the failover connection. They also have around 500+ employees who will need to use this connection. Which of the following connection types would you use?


Site-to-Site for the main and failover connection.


Site-to-Site for the main and Point-to-Site for the failover connection.


ExpressRoute for the main connection and Site-to-Site for the failover connection.


Site-to-Site for the main and ExpressRoute for the failover connection.

Explanation

An ExpressRoute connection behaves like a dedicated connection between your on-premise data center and Azure**.** You can establish multiple connections betweenyour on-premise data center and Azure. In the failover connection, since the company does not mind a drop in latency, they can opt for a Site-to-Site VPN connection. This type of model is often used for a primary and failover connection from on-premise data centers and Azure**.**


https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager
#16

You're an Azure Administrator who is tasked with configuring Azure DNS zones for your Azure AD tenant. You need to ensure that you can perform different types of resolutions for the Internet and the Intranet users when they use the same domain name. How can you accomplish this?


Reverse DNS


Private DNS

✗
Create a CName

✓
Split-Horizon

Explanation

A split-horizon DNS realizes different resolutions for the same DNS zone, provided whether you are inside Azure's networks or out on the internet.

https://docs.microsoft.com/en-us/azure/dns/private-dns-scenarios
#17

You are an Azure Engineer who has been tasked with deploying six virtual machines to a vNet subnet. Each VM needs both a public and a private IP address. The Network Security Group rules for each VM will be the same. What is the minimum number of network interfaces that will be needed to do this?

✗
12

✗
18

✓
6

✗
3

Explanation

One network interface provides both a private and public IP address for a virtual machine. Because there are six VMs, each requiring both private and public IP addresses, you only need six network interfaces.

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface
#18

There are four replicas of a multi-tier application separated into four resource groups with the following specifications:Each resource group is in a separate region - East US, West US, West Central US, and South Central US.Each resource group includes a replica of a three-tier application replica comprised of five VMs: Two front-end VMs, two mid-tier application VMs, and one back-end database VM.You would like to configure Azure network resources to accomplish the following:Route inbound requests to the application replica with the least network latency.Create a front-end firewall for all incoming requests from the internetEncrypt all traffic throughout communication between different application layers.Load balance incoming requests from the public internet, as well as requests between each tier of the application.Monitor the performance of each VM in each application tierWhich Azure network resource is not required to achieve these design requirements?


Azure Traffic Manager


Azure Application Gateway


Public Load Balancers


Internal Load Balancers

Explanation

Traffic Manager can distribute traffic at a DNS level to the respective application in each region based on estimated latency with performance routing. The application gateway can provide end-to-end SSL and health monitoring. It does not require additional load balancers to connect to the middle and back-end tiers of the application.

https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-end-to-end-ssl-powershell#create-a-public-ip-address-for-the-front-end-configuration
#19

You're an Azure engineer responsible for scaling on your company's newly deployed, multitier web application. Your company is expecting this site will be heavily trafficked as soon as it goes public, so you need to ensure the infrastructure is as robust and resilient as possible.The application consists of the following layers:Web Tier - User interfaceBusiness Tier - Logic to process user interactionsData Tier - Stores application dataSelect 3 appropriate configurations/services that would help scale your application.

✓ Deploy the app in at least two regions

✓ Place an Application Gateway in front of the app and use as a public endpoint for Traffic Manager

✓ Use a load balancer between the web tier and business tier

✗ Place a load balancer in front of the application

Explanation

Application Gateways can be used to scale application traffic, and thus should be utilized in front of the entire application. Deploying your app to multiple regions additionally increases scalability, so this can be used in tandem with the application gateways. A load balancer can also use health probes to monitor the availability of VM instances, and thus can be used to decouple application tiers and increase availability.

Cookie-based sessions are already enabled via the Application Gateway / Traffic Manager.

https://docs.microsoft.com/en-us/azure/architecture/high-availability/reference-architecture-traffic-manager-application-gateway

#20

Your company is looking to deploy a new application on a fleet of Azure VMs in the vNet referred to as “vNet3.” Your boss needs you to ensure the application is scalable and robust. Their requirements include:Path-based loading at the global level Traffic is load-balanced in vNet3100% TLS/SSL offload HTTP requests are routed within vNet3 Session affinity is supportedWhich actions should you take to meet these requirements? (Select 2).

✓ Place an Application Gateway in front of the VMs in vNet3

✓ Enable Azure Front Door

✗ Enable Azure Firewall

Enable Azure Traffic Manager

Explanation

Both the Application Gateway and Azure Front Door fulfill these requirements in tandem with each other; Azure Firewall does not deal with scaling but rather the security piece. Traffic Manager does not support session affinity. Global load balancing would not balance specifically in vNet3.

 https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq

#21

You want to connect the Azure VNets for three separate branch offices. You are designing a hub and spoke model network topology to do this. The central hub will serve as a firewall between the different locations during backend communication, and also a central location for disaster recovery backup storage. Now you are considering whether to connect your hub-and-spoke model with VNet peering connections or Azure VPN Gateways. Each option has its own benefits. Which statements comparing VNet peering and VPN Gateways in a hub-and-spoke model are correct? (Choose 2 answers)

If you implement the model with Azure VPN Gateways, all VNets **can be cross-region.**

If you implement the model with VNet peering connections, the VNets **can be cross-region with Global VNet Peering.**

Whether the connections are made with Azure VPN Gateways or VNet peering connections, the VNets can be **within different Azure subscriptions** and associated **with separate Azure AD tenants**.

If you implement the model with Azure VPN Gateways, all VNets **can be in different regions**.

If you implement the model with VNet peering connections, the VNets **must be in the same region**.

If you implement the model with Azure VPN Gateways, the VNets can be **within different Azure subscriptions** that are **associated with the same Azure tenant.**

If you implement the VNets with VNet peering connections, the VNets can be **within different Azure subscriptions** and **associated with separate Azure AD tenants**.

Explanation

You could accomplish this network topology using VNet peering or Azure VPN Gateways, but each option has its requirements and limitations.

1. Connecting via VNet peering would require a router to be deployed in the central hub VNet, but this is not required for VNG connections.
2. VNet peering works both across separate tenants and subscriptions.
3. Hostname resolution is not possible for VMs connecting from different VNets through a peering connection. Azure DNS is required for these VMs to connect. However, name resolution is possible through a VNG connection.
4. VNets must be connected via Global VNet Peering.

/course/azure-network-connectivity-name-resolution/virtual-network-peering/

Covered in this lecture
Virtual Network Peering
Course:Azure Network Connectivity and Name Resolution

4m
#22

A company has deployed two Azure Load Balancers to its Azure subscription. Load Balancer A has a basic SKU and Load Balancer B has a Standard SKU. Both Load Balancers A and B must balance requests across three VMs. How can you ensure Load Balancer B is balancing requests appropriately?

✗
Ensure the VMs are running in the same Azure region as Load Balancer B

✗
Ensure the VMs are created in the same resource group as Load Balancer B

✗
Ensure the VMs are using the same security group as Load Balancer B

✓
Ensure the VMs are created in the same virtual network as Load Balancer B

Explanation

When using Standard Load Balancers, VMs must be a part of a single virtual network. This vNet must be the same as the one hosting the VMs.

https://docs.microsoft.com/en-us/azure/load-balancer/skus

#23

You have a two-tier application hosted within VNet-01 with an IP address range of 10.0.1.0/16 and the following resource configurations: A web application front end hosted on an IaaS virtual machine named VM_Front within a public subnet with an IP address range of 10.0.2.0/24. VM_Front has a private IP address of 10.0.2.5, and a public IP address of 192.168.50.2. A web application backend hosted on a second IaaS virtual machine named VM_Back within a private subnet with an IP address range of 10.0.3.0/24. VM_Back has a private IP address of 10.0.3.4. A public-facing load balancer with a private IP address of 10.0.1.6 and a public IP address of 172.16.50.35. You are configuring the network security group for VM_Front, and want it to receive encrypted HTTP traffic from the load balancer, and want this to be one of the first rules the NSG processes against all incoming traffic. How would you configure a rule to allow this?

Inbound Rule

Source: 10.0.1.6

Source Port: *

Destination: 10.0.2.5

Destination Port: 443

Protocol: TCP

Priority: 100

Action: Allow

Inbound Rule

Source: 10.0.2.5

Source Port: 80

Destination: 172.16.50.35

Destination Port: *

Protocol: UDP

Priority: 100

Action: Allow

Inbound Rule

Source: 10.0.1.6

Source Port: *

Destination: 10.0.3.4

Destination Port: 8080

Protocol: TCP

Priority 5000

Action: Allow

Inbound Rule

Source: 10.0.2.5

Source Port: *

Destination: 10.0.3.4

Destination Port: 443

Protocol: HTTPS

Priority: 9999

Action: Allow

Explanation

The correct rule parameters are:

- **Inbound Rule**
- **Source: 10.0.1.6**
- **Source Port: ***
- **Destination: 10.0.2.5**
- **Destination Port: 443**
- **Protocol: TCP**
- **Priority 100**
- **Action: Allow**

/course/implementing-azure-network-security/configuring-security-rules-in-an-nsg/

#24

You are designing your company's virtual networks and must consider ways to control costs and design for high availability. Your company has several general cost-saving rules in place, but your current design may be an exception. If resources need to remain available in the event of a complete data center outage, which of these cost-saving rules would you need to break?

Peer VNets only when necessary

Keep resources within one region as much as possible

Design multi-regional deployments to be regionally independent

Favor availability sets deployments rather than multi-availability zone deployments

Explanation

For your resources to remain available in the event of a complete data center outage, you should deploy them in multiple availability zones rather than within an availability set.

/course/optimizing-azure-costs/optimize-network-costs/?

context_id=390&context_resource=lp
Covered in this lecture

Optimize Network Costs
Course:Optimizing Azure Costs

6m

#25

You're conducting a security audit on a new Azure application that is hosted on virtual machines deployed in a virtual network called VNetApp1. The application should ONLY have access to Azure SQL resources in the East US Azure region. Which outbound network security group (NSG) rule(s) should be present to ensure the application has the appropriate access? Select the 3 answer choices that apply.

✓ A deny rule with a source of VirtualNetwork and a destination of 0.0.0.0/0

✗ An allow rule that has the IP address range of VNetApp1 as the source and destination of Sql.EastUS

✓ A deny rule that has the IP address range of VNetApp1 as the source and the destination of 168.63.129.0/24

✓ An allow rule that has the source of Sql.EastUS and destination of the IP address range of VNetApp1

Explanation

The virtual network should not have access to the internet, as the question specifies that it only needs access to the SQL resources. A deny rule with a source of VirtualNetwork and a destination of 0.0.0.0/0 reflects this requirement, so this is correct. The network additionally should not have access to any other Azure resources, which are always located in IP address 168.63.129.0/24. Lastly, An allow rule that has the source of Sql.EastUS and destination of the IP address range of VNetApp1 must be present to ensure access to the appropriate SQL resources.

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works