Module 2: Azure Networking

Exercise 1: Configure Azure Networking

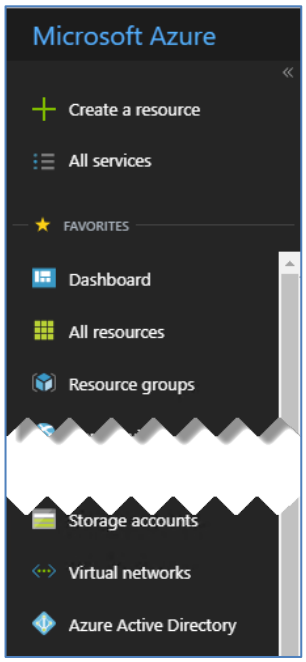
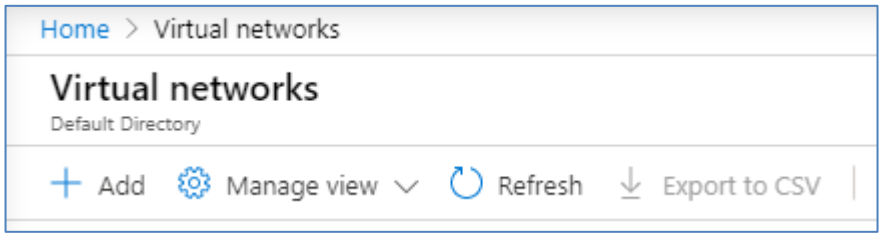
In this exercise, you prepare the Azure Virtual Network (VNet) for NetApp Cloud Manager (Cloud Manager) and NetApp Cloud Volumes ONTAP software deployments. This preparation includes creating a VNet, subnets, and network security groups.

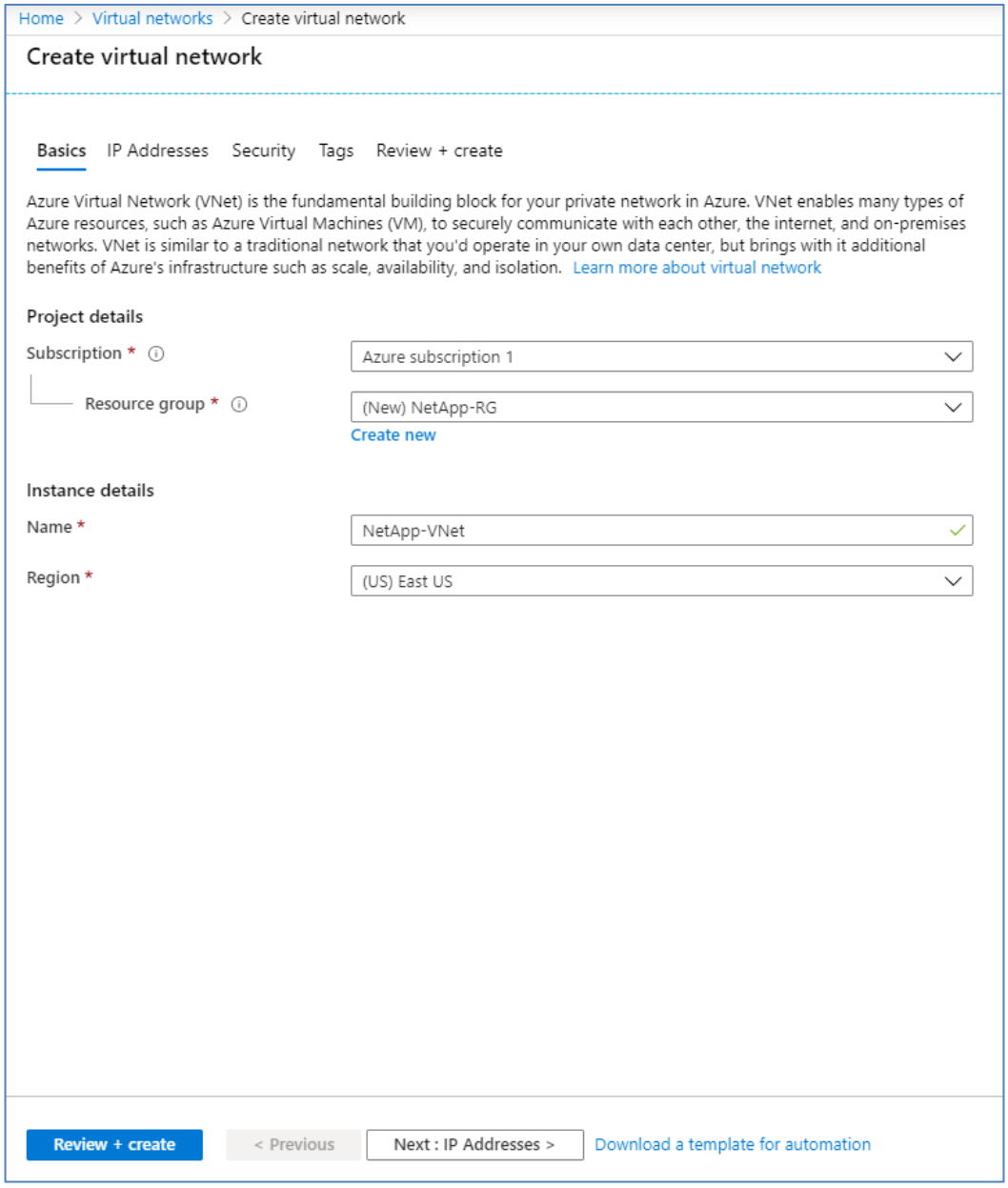
Objectives

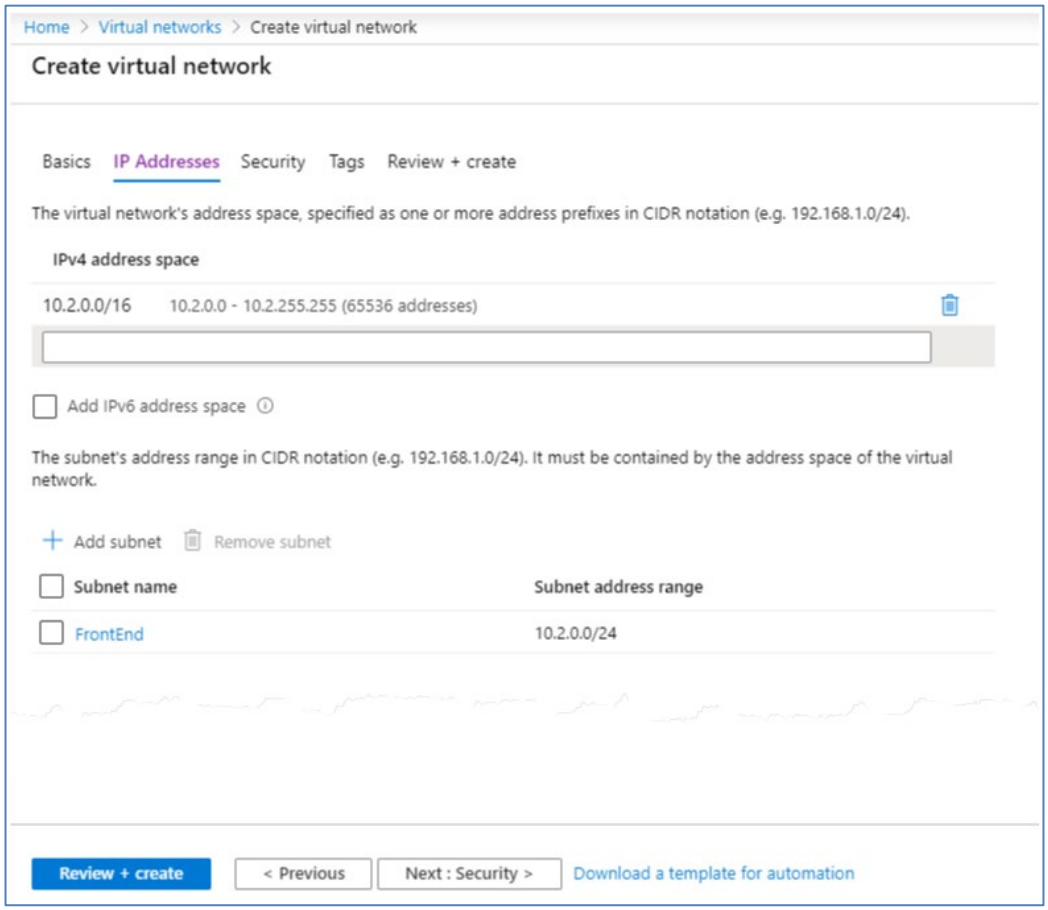
This exercise focuses on enabling you to do the following:

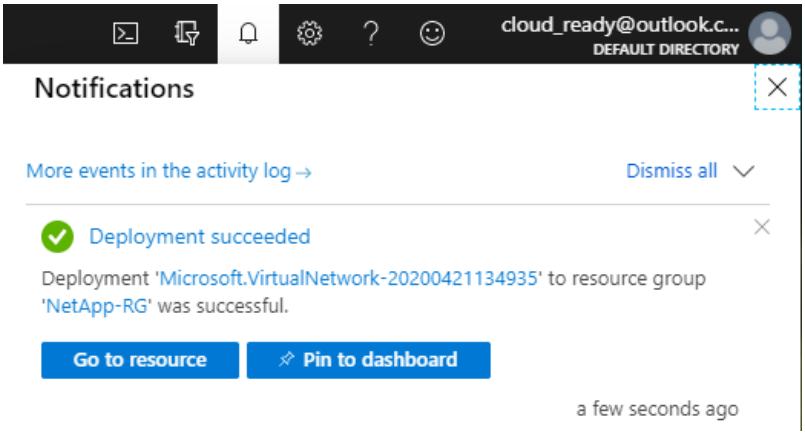
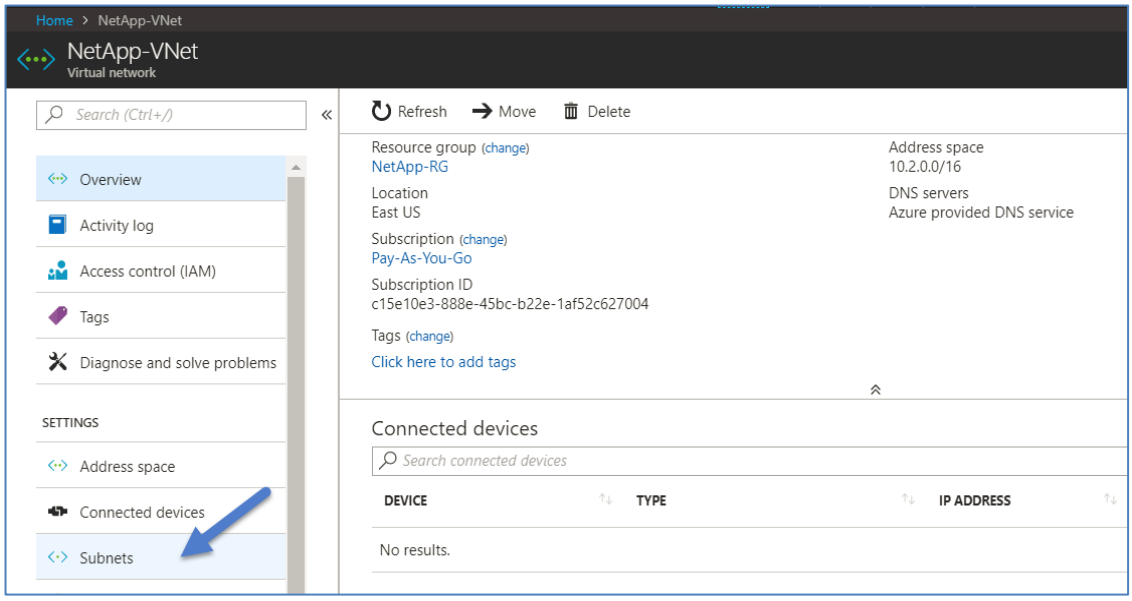
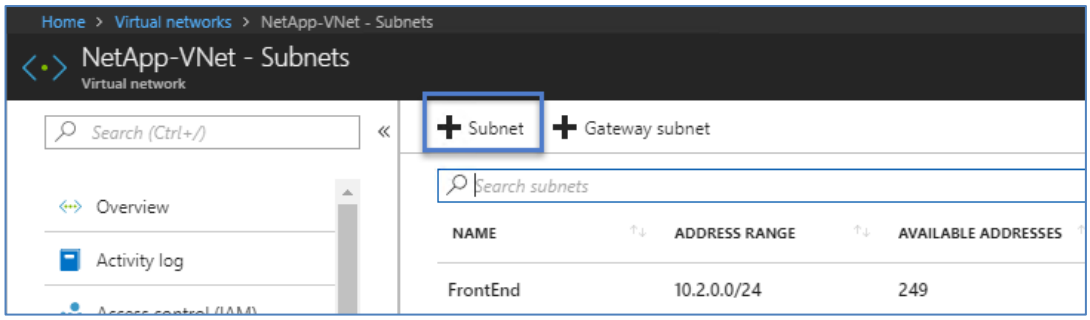
- Create an Azure VNet with a front-end subnet and a back-end subnet.
- Create and apply security groups to subnets.

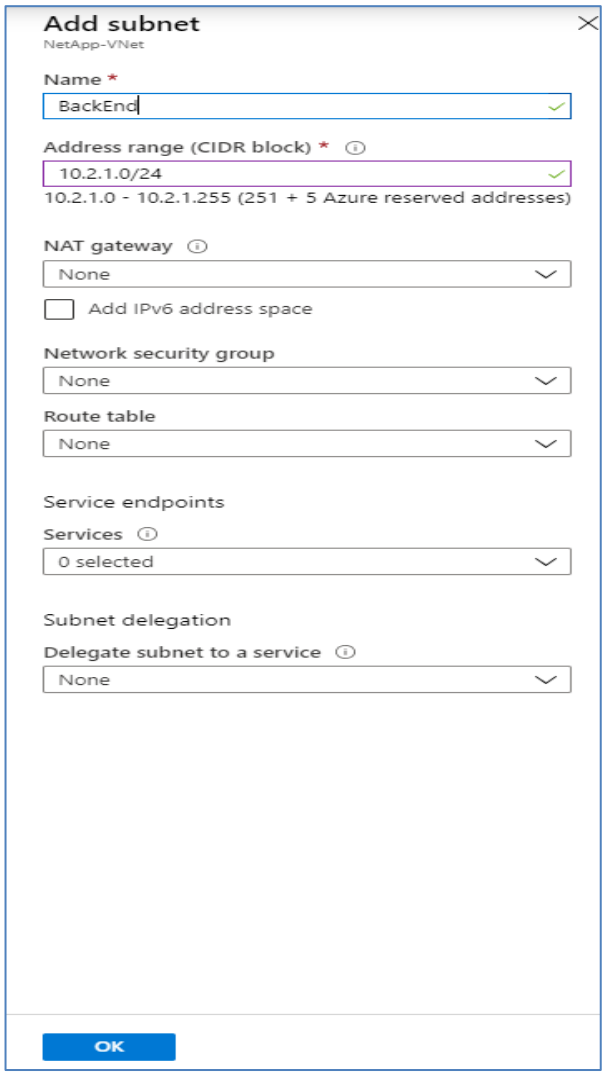
Task 1: Create an Azure VNet and Azure Subnets

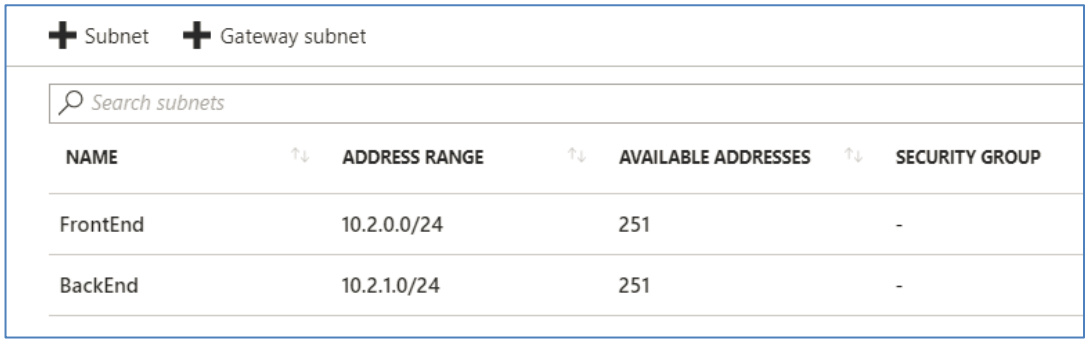
Step	Action
1-1	Open a web browser and enter the URL **https://portal.azure.com**.
1-2	On the Favorites menu, click **Virtual networks**. 
1-3	In the Virtual networks blade (pane), click +**Add**. 

Step	Action
1-4	In Create virtual network under Basics, do the following: a. For the Subscription, make sure your subscription is selected. b. For the Resource Group, select **Create new**, and enter **NetApp-RG**. c. For the Instance details, next to Name, enter **NetApp-VNet**. d. For the Region, click the drop-down menu and select **(US) East US**. e. Click **Next: IP Addresses**. 

Step	Action
1-5	In Create virtual network under IP Addresses, do the following: a. For the IPv4 Address space, remove the default and enter **10.2.0.0/16**. b. For the subnet, click **+ Add subnet**, then enter the subnet name **FrontEnd.** c. For the Subnet address range, enter **10.2.0.0/24**. d. Click **Add**. e. Retain the rest of the default values. f. Click **Review + Create**. 
1-6	After validation passes, click **Create**.

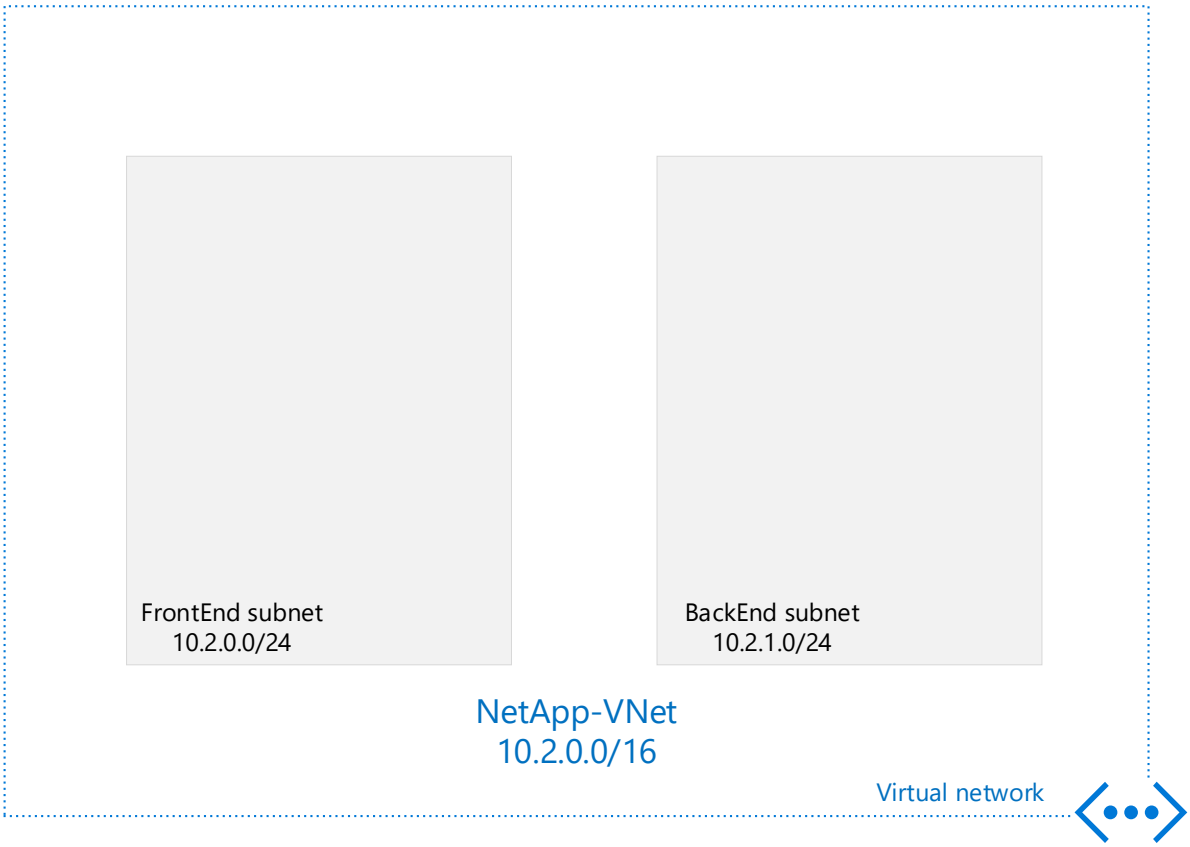
Step	Action
1-7	In the top toolbar, click the **Notifications** bell, wait for the deployment to finish, and when the deployment is complete, click **Go to resource**. 
1-8	In the NetApp-VNet blade, click **Subnets**. 
1-9	In the NetApp-VNet – Subnets blade, click **+Subnet**. 

Step	Action
1-10	Under Add subnet, do the following: a. For the Name, enter **BackEnd**. b. For the Address range (CIDR block), enter **10.2.1.0/24**. c. Retain the rest of the default values. d. Click **OK**. 
1-11	QUESTION: Are there any restrictions on using IP addresses within these subnets? Yes. Azure reserves some IP addresses within each subnet. The first and final IP addresses of each subnet are reserved for protocol conformance, and the x.x.x.1-x.x.x.3 addresses of each subnet are used for Azure services.
1-12	Azure provides sufficient default routes, so no explicit route table is configured. For information about Azure default routes, see this link: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#default

Step	Action
1-13	Verify that the subnet is added. 

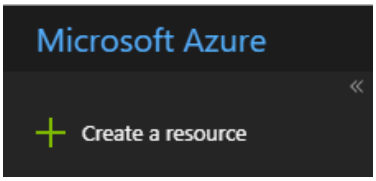
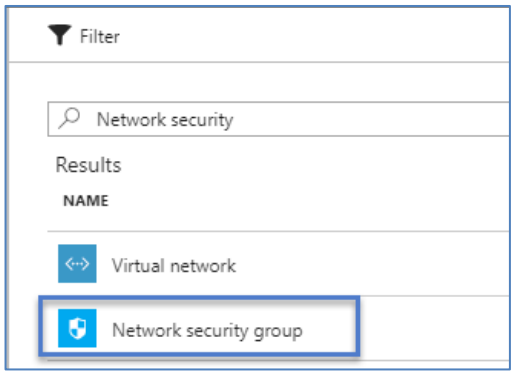
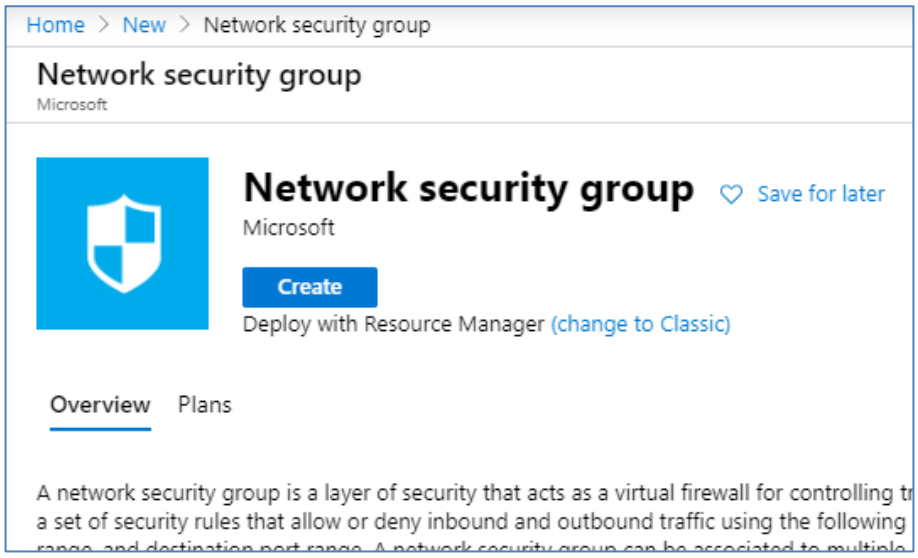
Azure Diagram

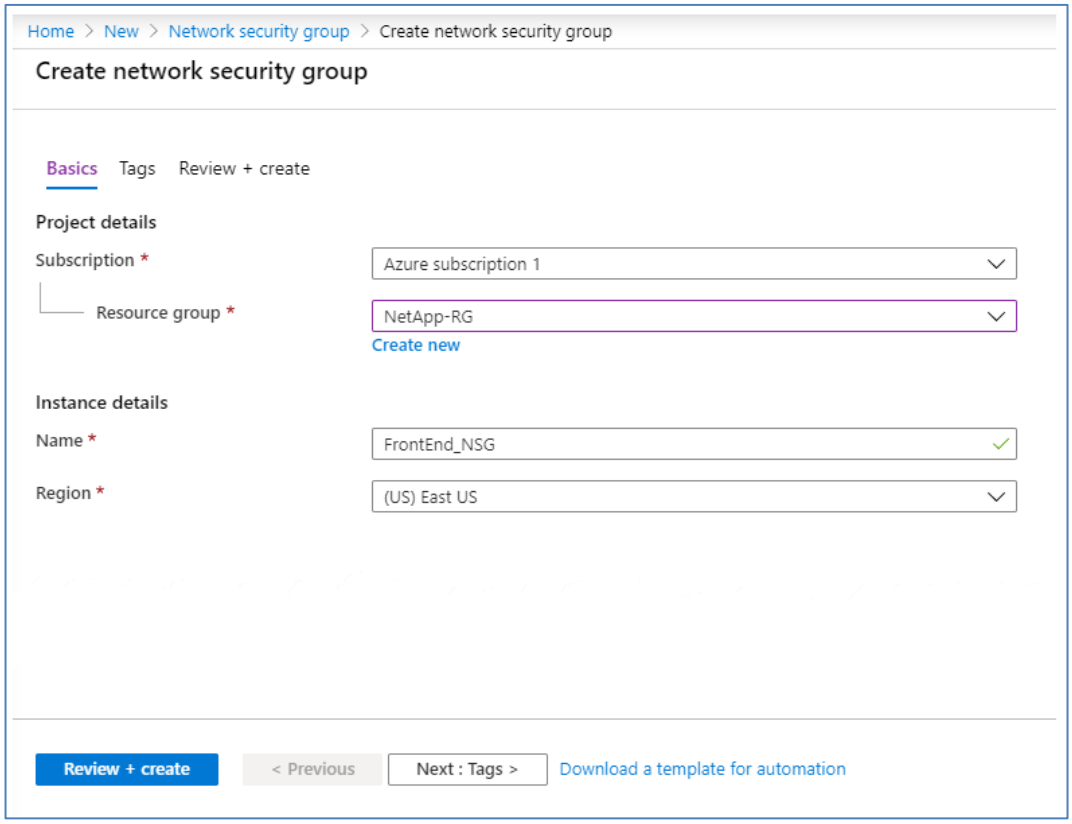
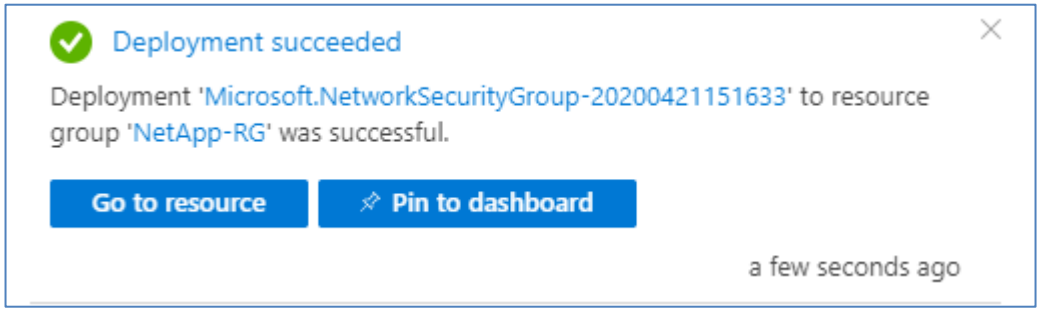
After you complete Task 1: Create an Azure VNet and Azure Subnets, the configuration of the Azure network is as displayed in the following figure.

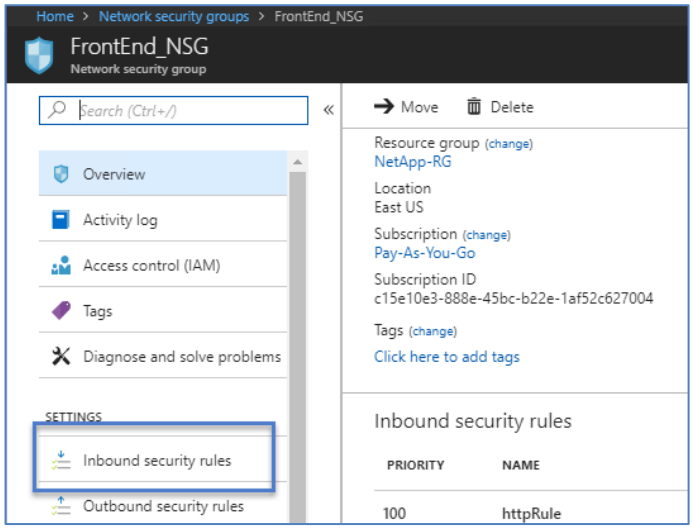
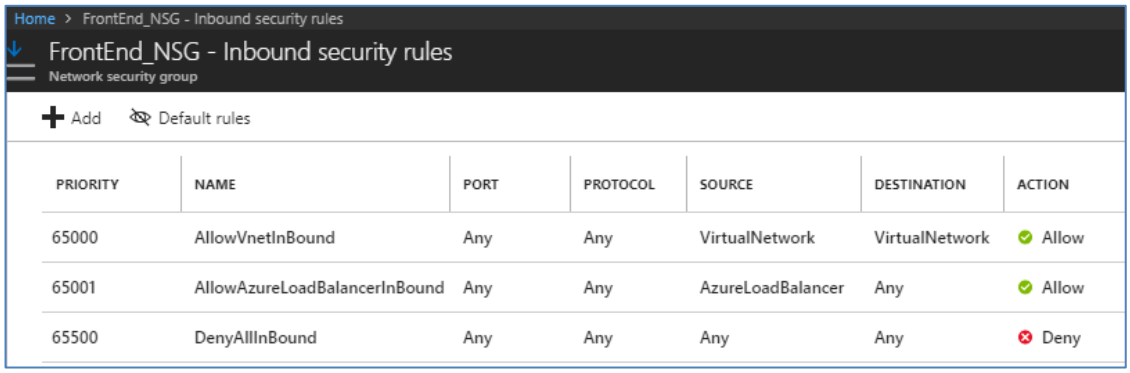


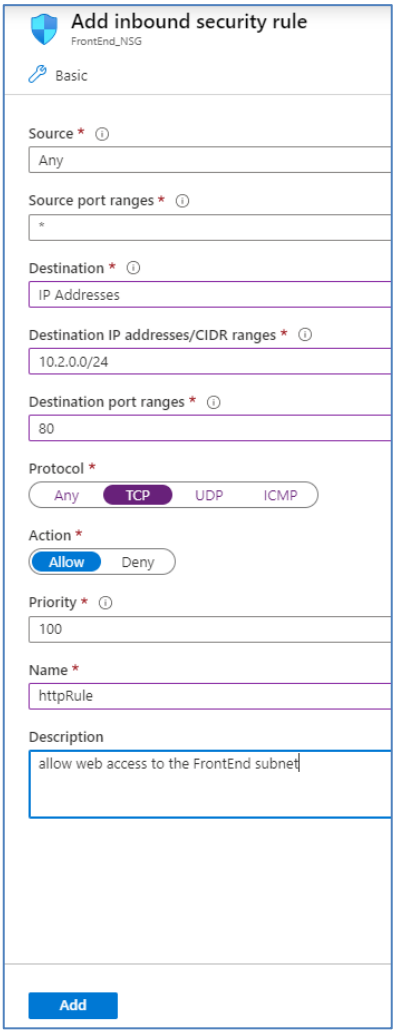
Task 2: Create Security Groups

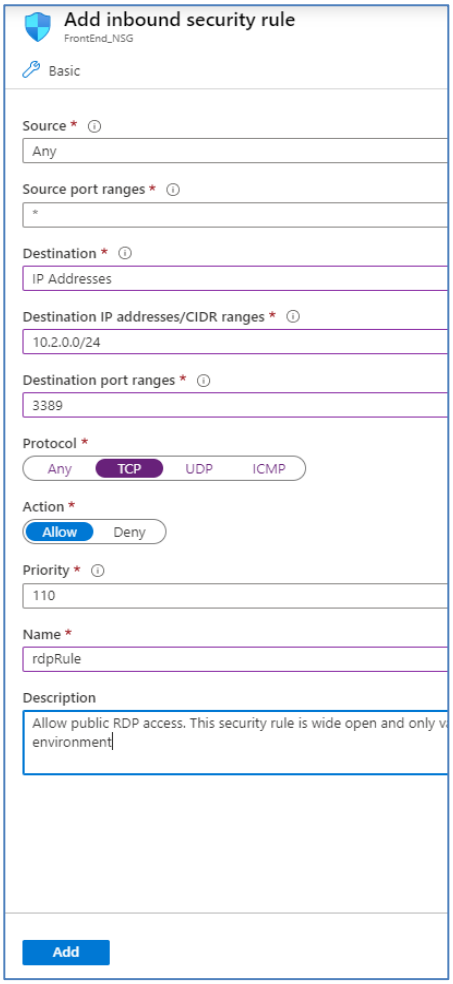
In this task, you create security groups for the FrontEnd (public facing) and BackEnd (private) subnets.

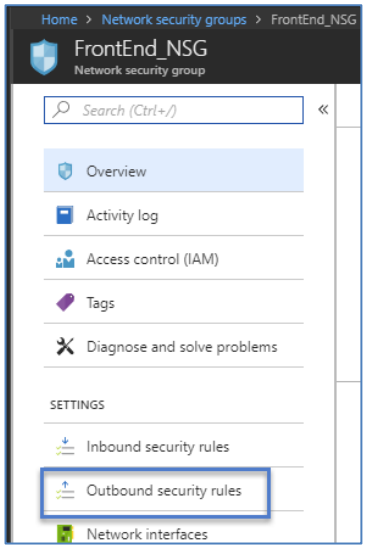
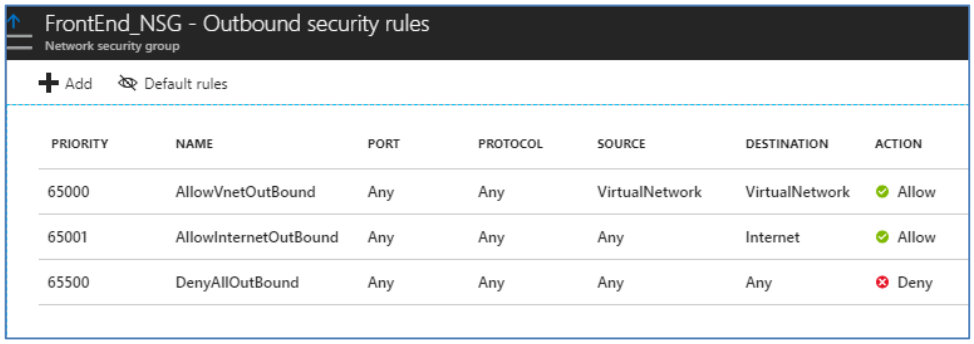
Step	Action
2-1	In the Azure portal, click + **Create a resource**. 
2-2	In the search box, type **Network security,** and select **Network security group**. Note: Do not select Network security groups (classic) 
2-3	In the Network security group blade, the Deploy with Resource Manager is already selected by default**,** click **Create**. 

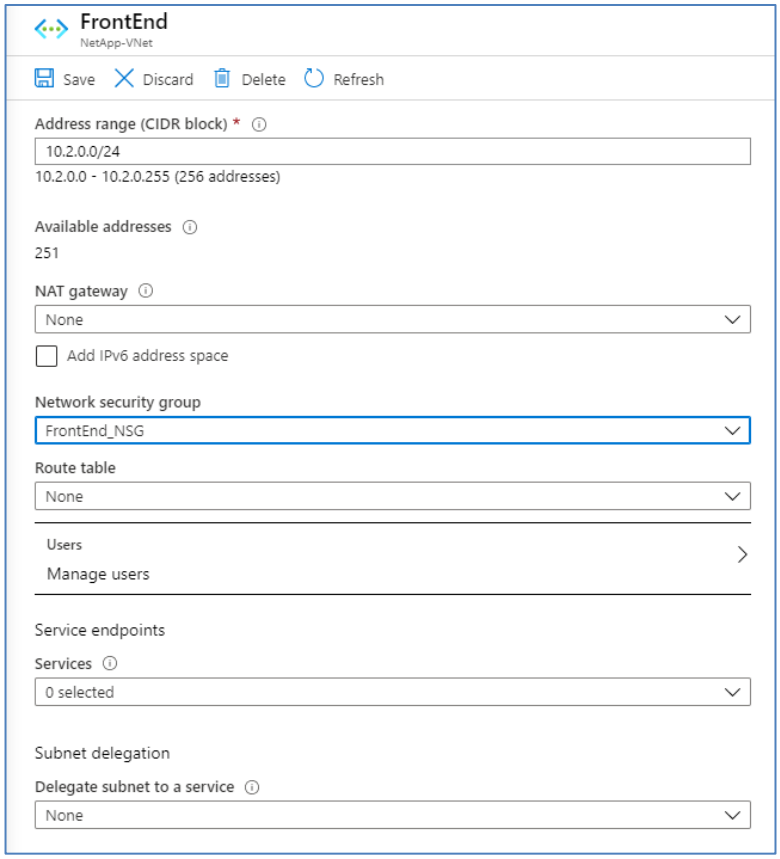
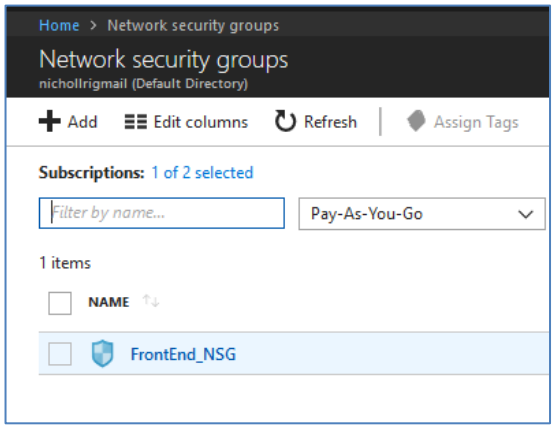
Step	Action
2-4	In the Create network security group under Basics, do the following: a. For the Subscription, make sure your subscription is selected**.** b. For the Resource group, click the drop-down menu, and select **NetApp-RG**. c. For the Name, enter **FrontEnd_NSG**. d. For the Location, select **East US** (default). e. Click **Review + Create**. 
2-5	After validation passes, click **Create**.
2-6	In the Notifications bell, monitor the deployment, and when the deployment is complete, click **Go to resource**. 

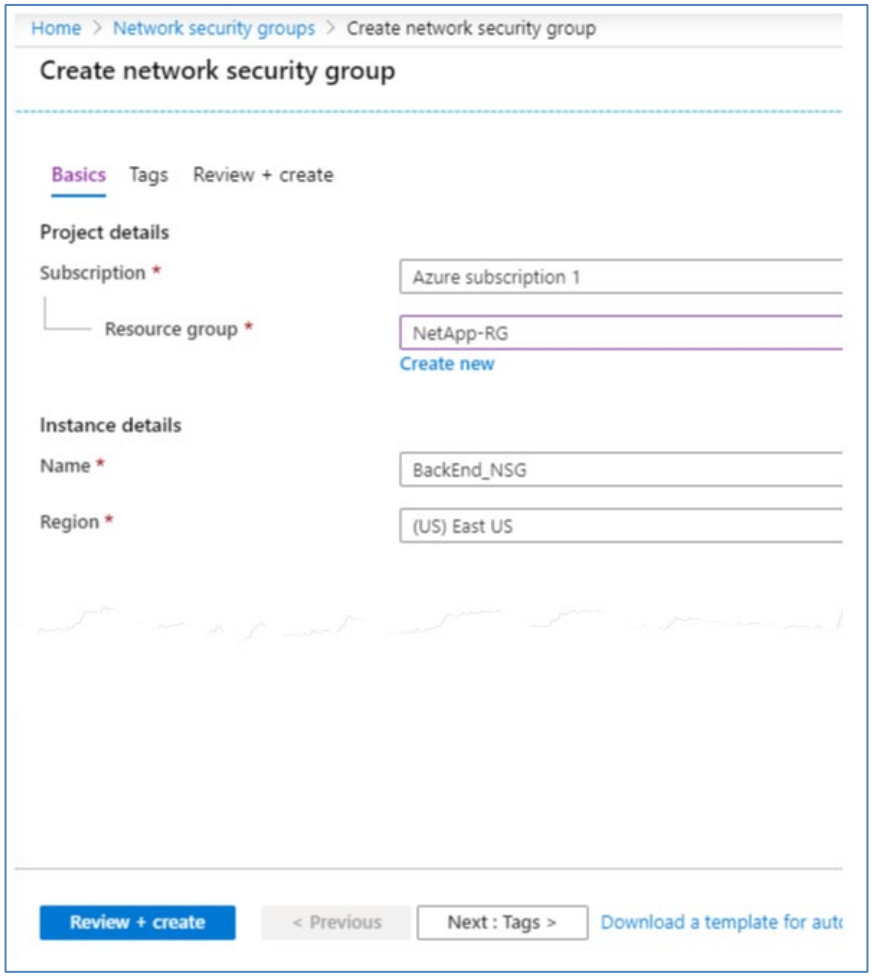
Step	Action
2-7	Under FrontEnd_NSG, click **Inbound security rules**. 
2-8	Under FrontEnd_NSG - Inbound security rules, verify that these three rules exist by default: 
2-9	Click +**Add**.

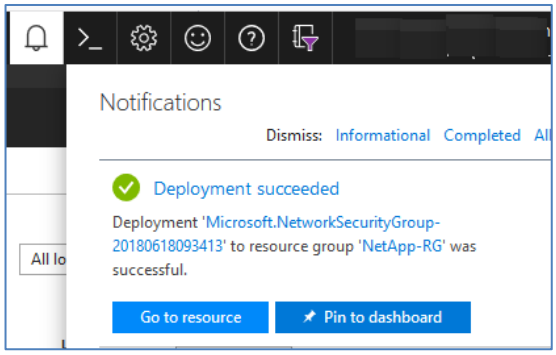
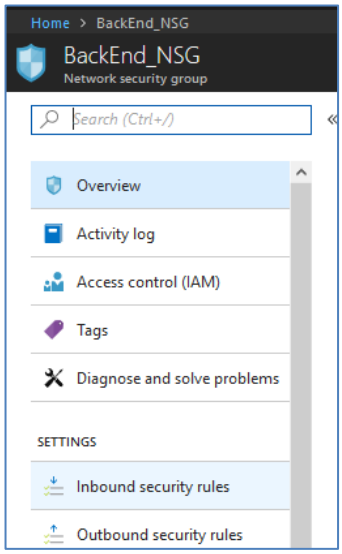
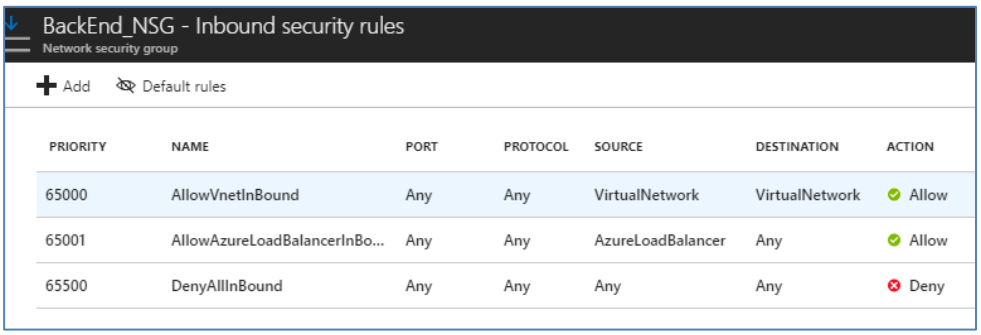
Step	Action
2-10	Under Add inbound security rule, do the following: a. For the Source, select **Any**. b. For the Source port ranges, the default is *****. c. For the Destination, select **IP Addresses**. d. For the Destination IP addresses/CIDR ranges, enter **10.2.0.0/24**. e. For the Destination port ranges, enter **80**. f. For the Protocol, select **TCP**. g. For the Action, the default is **Allow**. h. For the Priority, enter **100**. i. For the Name, enter **httpRule**. j. For the Description, enter **allow web access to the FrontEnd subnet**. k. Click **Add**. 
2-11	Under FrontEnd_NSG - Inbound security rules, click **+Add** to create a second rule.

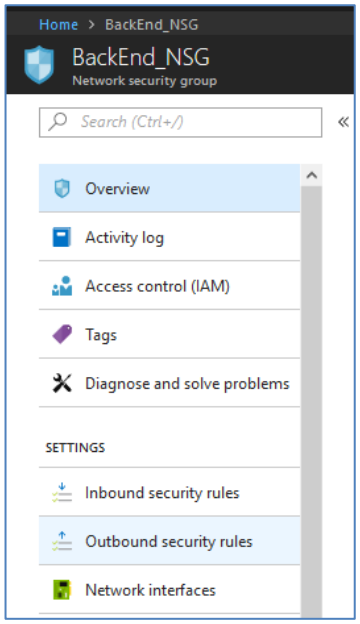
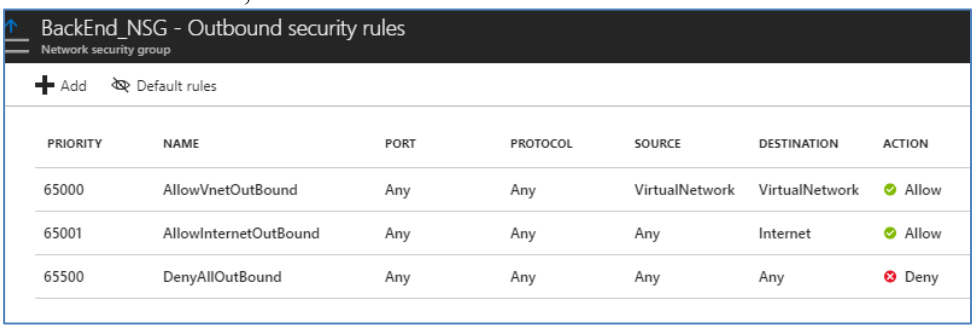
Step	Action
2-12	Under Add inbound security rule, do the following: a. For the Source, select **Any**. b. For the Source port ranges, the default is *****. c. For the Destination, select **IP Addresses**. d. For the Destination IP addresses/CIDR ranges, enter **10.2.0.0/24**. e. For the Destination port ranges, enter **3389**. f. For the Protocol, select **TCP**. g. For the Action, the default is **Allow**. h. For the Priority, enter **110**. i. For the Name, enter **rdpRule**. j. For the Description, enter **Allow public RDP access. This security rule is wide open and only valid for a demo environment**. k. Click **Add**. 
2-13	Verify you have successfully added two new Inbound security rules for HTTP and RDP by clicking the **Refresh** button. 

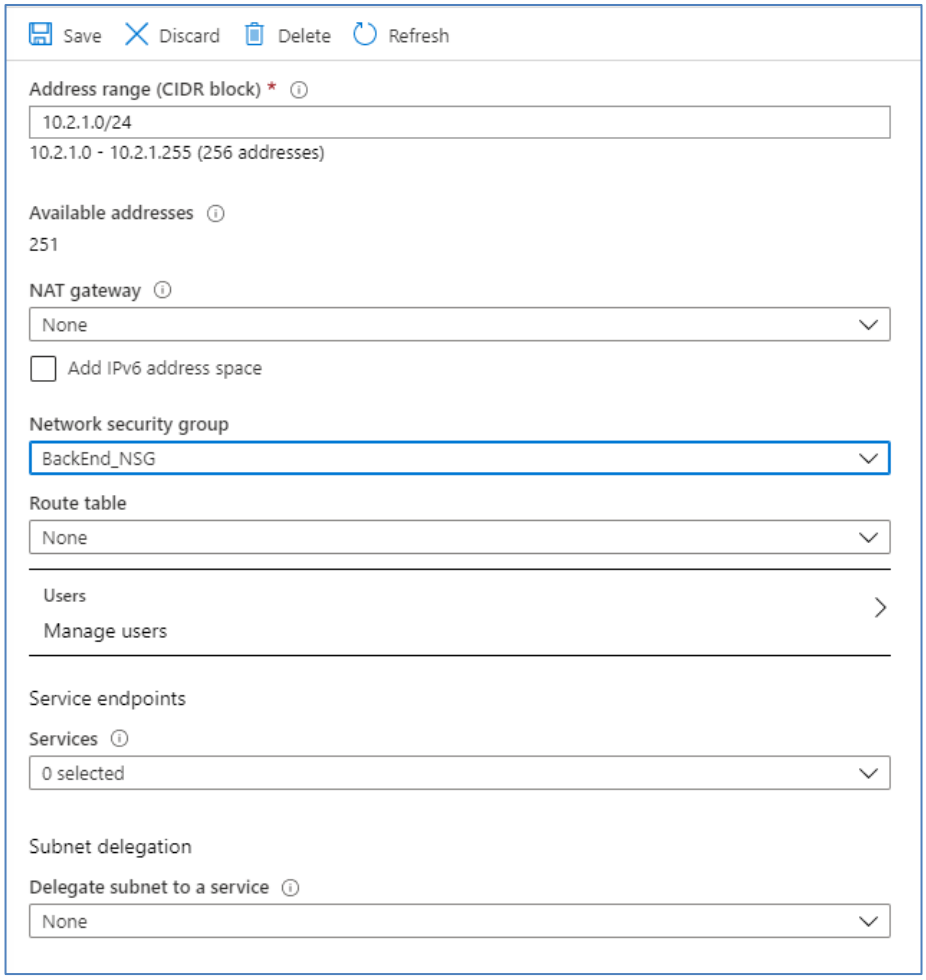
Step	Action
2-14	Under FrontEnd_NSG, click **Outbound security rules**. 
2-15	With the AllowInternetOutbound rule, all network traffic that is outbound to the internet is allowed.  PRIORITY / NAME / PORT / PROTOCOL / SOURCE / DESTINATION / ACTION 65000 / AllowVnetOutBound / Any / Any / VirtualNetwork / VirtualNetwork / Allow 65001 / AllowInternetOutBound / Any / Any / Any / Internet / Allow 65500 / DenyAllOutBound / Any / Any / Any / Any / Deny
2-16	Click the **X** to close the FrontEnd_NSG Outbound security rules blade.
2-17	To attach the FrontEnd_NSG network security group to the FrontEnd subnet, in the Azure portal, select **Virtual networks** > **NetApp-VNet** > **Subnets.**
2-18	Click the **FrontEnd** row.

Step	Action
2-19	In the FrontEnd blade, click the drop-down menu for **Network security group** and click **FrontEnd_NSG**. 
2-20	Click **Save**.
2-21	In the search box, type **Network security**, and select **Network security groups**.
2-22	In the Network security group blade, click **Add**. 

Step	Action
2-23	Under Create network security group, do the following: a. For the Subscription, select make sure your subscription is selected. b. For the Resource Group, select **the drop-down menu**, then select **NetApp-RG**. c. For the Name, enter **BackEnd_NSG**. d. For the Location, select **East US**. (default) e. Click **Review + Create**. 
2-24	After Validation passed, click **Create**.

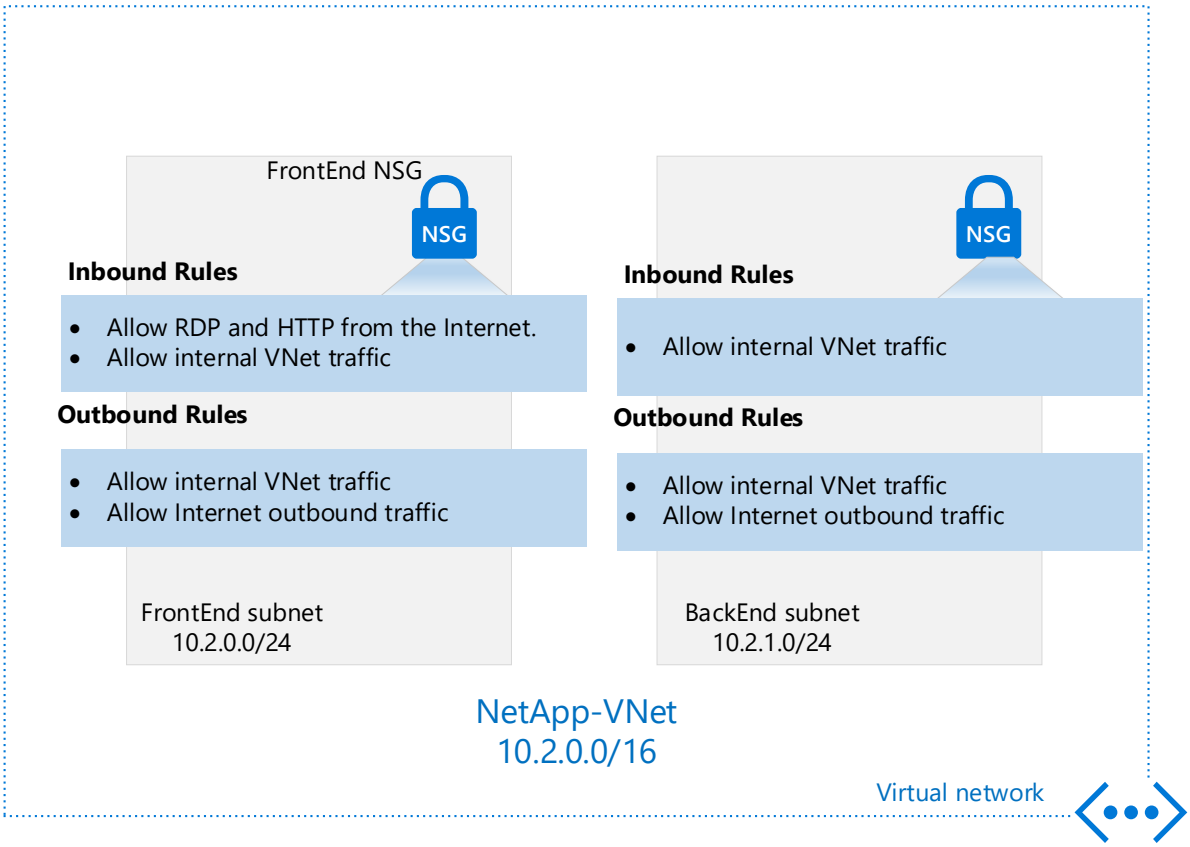
Step	Action
2-25	In the top toolbar, click the **Notifications** bell, monitor the deployment, and when the deployment is complete, click **Go to resource**. 
2-26	Under BackEnd_NSG, click **Inbound security rules**. 
2-27	No rules allow internet inbound access. The two Allow rules allow inbound access from within the VNet and from Azure Load Balancers. All other traffic is denied.  PRIORITY / NAME / PORT / PROTOCOL / SOURCE / DESTINATION / ACTION 65000 / AllowVnetInBound / Any / Any / VirtualNetwork / VirtualNetwork / Allow 65001 / AllowAzureLoadBalancerInBo... / Any / Any / AzureLoadBalancer / Any / Allow 65500 / DenyAllInBound / Any / Any / Any / Any / Deny

Step	Action
2-28	Under BackEnd_NSG, click **Outbound security rules**. 
2-29	Default security rules allow outbound traffic within the VNet and allow outbound traffic to the internet, so the default rules are sufficient.  PRIORITY / NAME / PORT / PROTOCOL / SOURCE / DESTINATION / ACTION 65000 / AllowVnetOutBound / Any / Any / VirtualNetwork / VirtualNetwork / Allow 65001 / AllowInternetOutBound / Any / Any / Any / Internet / Allow 65500 / DenyAllOutBound / Any / Any / Any / Any / Deny
2-30	In a later exercise, Cloud Volumes ONTAP is deployed in the BackEnd subnet. You configured the outbound rules that adhere to the networking requirement: • Cloud Volumes ONTAP requires outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage. • Routing and firewall policies must allow Azure HTTP and HTTPS traffic to mysupport.netapp.com so that Cloud Volumes ONTAP can send AutoSupport messages.
2-31	To attach the BackEnd_NSG network security group to the BackEnd subnet, in the Azure portal, select **Virtual networks** > **NetApp-VNet** > **Subnets.**
2-32	Click the **BackEnd** row.

Step	Action
2-33	In the BackEnd blade, click the drop-down menu for **Network security group,** then select **BackEnd_NSG**. 
2-34	Click **Save**.

Azure Diagram

After you complete Task 2: Create Security Groups, the configuration of the Azure network is as displayed in the following figure.



End of Exercise