

Configure Network Security to Allow Application Traffic

Understand the scenario

You are an Azure® administrator. You need to configure a secure network that contains multiple Azure virtual machines in a multi-tier architecture. First, you will create a virtual network for each tier, and then you will implement peering for internal communication. Next, you will create a virtual machine for each tier. Finally, you will configure a network security group (NSG) for the web tier, and then you will test the configuration.

Understand your environment

You will be using an Azure resource group named corp-datalod26433816 that contains no resources.

# **Configure peering between virtual networks**

* Sign in to the Azure portal
* Create a virtual network for the web tier by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433816** |
| Name | webVNET |
| IPv4 address space | 10.10.0.0/16 |
| Subnet name | web |
| Subnet address range | 10.10.0.0/25 |

* Expand this hint for guidance on creating virtual networks.
  + Review the documentation on [creating virtual networks](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal#create-virtual-networks).
* Create a virtual network for the application tier by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433816** |
| Name | appVNET |
| IPv4 address space | 10.20.0.0/16 |
| Subnet name | app |
| Subnet address range | 10.20.0.0/25 |

* Create a virtual network for the database tier by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433816** |
| Name | dbVNET |
| IPv4 address space | 10.30.0.0/16 |
| Subnet name | db |
| Subnet address range | 10.30.0.0/25 |

* Create virtual network peering connections from webVNET to **appVNET** by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| This virtual network - Peering link name | webVNET-to-appVNET |
| Remote virtual network - Peering link name | appVNET-to-webVNET |
| Virtual network | **appVNET** |

* Expand this hint for guidance on creating peering connections between virtual networks.
  + Review the documentation on [peering virtual networks](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal#peer-virtual-networks).
* Create virtual network peering connections from appVNET to **dbVNET** by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| This virtual network - Peering link name | appVNET-to-dbVNET |
| Remote virtual network - Peering link name | dbVNET-to-appVNET |
| Virtual network | **dbVNET** |

## Check your work

Verify that you have created three virtual networks named webVNET, appVNET, and dbVNET.

Verify that you have created two peering connections between webVNET and appVNET.

Verify that you have created two peering connections between appVNET and dbVNET.

# **Create Azure virtual machines for a multi-tier app**

* Create an Azure virtual machine for the web tier by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433816** |
| Virtual machine name | webVM1 |
| Image | **Windows Server 2019 Datacenter - Gen1** |
| Size | **Standard\_B2ms - 2 vcpus 8 GiB memory** |
| Username | AzureAdmin |
| Password | Az!26433816! |
| Virtual network | **webVNET** |
| Subnet | **web (10.10.0.0/25)** |
| Boot diagnostics | **Disable** |

* Expand this hint for guidance on creating a virtual machine.
  + Review the documentation on [creating a virtual machine](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal#create-virtual-machines).
* Create an Azure virtual machine for the application tier by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433816** |
| Virtual machine name | appVM1 |
| Image | **Ubuntu Server 18.04 LTS - Gen1** |
| Size | **Standard\_B2ms - 2 vcpus 8 GiB memory** |
| Authentication type | **Password** |
| Username | AzureAdmin |
| Password | Az!26433816! |
| Virtual network | **appVNET** |
| Subnet | **app (10.20.0.0/25)** |
| Boot diagnostics | **Disable** |

* Create an Azure virtual machine that hosts SQL Server 2019 on Windows Server 2019 by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433816** |
| Virtual machine name | dbVM1 |
| Image | **Free SQL Server License: SQL 2019 Developer on Windows Server 2019 - Gen1** |
| Size | **Standard\_B2ms - 2 vcpus 8 GiB memory** |
| Username | AzureAdmin |
| Password | Az!26433816! |
| Virtual network | **dbVNET** |
| Subnet | **db (10.30.0.0/25)** |
| Boot diagnostics | **Disable** |
| SQL connectivity | **Private (within Virtual Network)** |
| SQL Authentication | **Enable** |

## Check your work

Verify that you have created a virtual machine named webVM1.

Verify that you have created a virtual machine named appVM1.

Verify that you have created a virtual machine named dbVM1.

# **Configure a network security group**

* Verify that the webVM1-nsg network security group (NSG) has an inbound security rule named **RDP** that allows RDP traffic into **webVM1**.

Expand this hint for guidance on working with network security groups.

* + Review the documentation on [working with network security groups](https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group#work-with-network-security-groups).
* Add an inbound security rule to the webVM1-nsg NSG to allow HTTP and HTTPS traffic by using the values in the following table. For any property that is not specified, use the default value.

| **Setting** | **Value** |
| --- | --- |
| Service | **Custom** |
| Destination port ranges | 80,443 |
| Action | **Allow** |
| Name | AllowAllweb |

* Expand this hint for guidance on creating security rules.
  + Review the documentation on [creating security rules](https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group#work-with-security-rules).
* Connect to webVM1 through **RDP** by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| IP address | **Public IP address** |
| Username | AzureAdmin |
| Password | Az!26433816! |

* On **webVM1**, run the following command in **Windows PowerShell** to install IIS:

Install-WindowsFeature -name web-Server -IncludeManagementTools

* Record the **Public IP address** of webVM1 in the following **Public IP Address** text box:

**Public IP Address**  


* Open a new browser window, and then go to the public IP address of WebVM1 at http://<PublicIP>.

You should see the default IIS webpage. This will verify that web traffic has been routed correctly by using a network security group.



## Check your work

Verify that you have added an inbound security rule named AllowAllweb to the webVM1-nsg NSG that allows HTTP and HTTPS traffic.

# **Summary**

Congratulations, you have completed the **Can You Configure Network Security to Allow Application Traffic?** challenge.

In this challenge, you have accomplished the following:

* Created Azure virtual networks.
* Implemented peering for internal communication between virtual networks.
* Created Azure virtual machines for a multi-tier app.
* Configured a network security group.
* Configured an inbound security rule to allow HTTP and HTTPS traffic.