

Configure Multi-Scope Network Security

Understand the scenario

You are an Azure® administrator. You need to create Azure virtual machines that use multi-scope network security. First, you will create a virtual network that includes two subnets, and then you will create a network security group. Next, you will create two virtual machines, one for each subnet. Finally, you will verify the network security configuration.

Understand your environment

You will be using an Azure resource group named corp-datalod26434344 that initially contains no resources.

# **Create an Azure virtual network that contains subnets and a network security group**

* Open Microsoft Edge, and then sign in to http://portal.azure.com
* Create a virtual network in the Azure portal by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26434344** |
| Name | webVNET |
| IPv4 address space | 10.10.0.0/16 |
| Subnet name | web |
| Subnet address range | 10.10.0.0/26 |

* Expand this hint for guidance on creating a virtual network.
  + Review the documentation on [creating a virtual network](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal" \l "create-virtual-networks" \o "Create virtual networks" \t "_blank).
* Add a subnet named admin to the webVNET virtual network to support the address range 10.10.1.0/26.

Expand this hint for guidance on adding a subnet.

* + Review the documentation on [adding a subnet](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet" \l "add-a-subnet" \o ).
* Create a network security group named webNSG in the **corp-datalod26434344** resource group.

Expand this hint for guidance on creating a network security group.

* + Review the documentation on [creating a network security group](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic" \l "create-a-network-security-group" \o "Create a network security group" \t "_blank).
* Associate the webNSG network security group to the **web** subnet in the **webVNET** virtual network.

Expand this hint for guidance on associating a network security group to a subnet.

* + Review the documentation on [associating a network security group to a subnet](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic" \l "associate-network-security-group-to-subnet" \o "Associate network security group to subnet" \t "_blank).

## Check your work

Verify that you have created a virtual network named webVNET.

Verify that you have created a network security group named webNSG.

Verify that you have associated the webNSG network security group to the web subnet.

# **Deploy an Azure virtual machine to each subnet**

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

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26434344** |
| Virtual machine name | VM1 |
| Image | **Windows Server 2019 Datacenter - Gen1** |
| Size | **Standard\_B2s - 2 vcpus 4GiB memory** |
| Username | AzureAdmin |
| Password | Az!26434344! |
| Public inbound ports | **None** |
| Virtual network | **webVNET** |
| Subnet | **web (10.10.0.0/26)** |
| NIC network security group | **None** |
| 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" \l "create-virtual-machines" \o "Create a virtual machine" \t "_blank).
* Record the public IP address of **VM1** in the following **Public IP Address** text box:

**VM1 Public IP Address**  


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

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26434344** |
| Virtual machine name | VM2 |
| Image | **Windows Server 2019 Datacenter - Gen1** |
| Size | **Standard\_B2s - 2 vcpus 4GiB memory** |
| Username | AzureAdmin |
| Password | Az!26434344! |
| Public inbound ports | **Allow selected ports** |
| Select inbound ports | **RDP (3389)** |
| Virtual network | **webVNET** |
| Subnet | **admin (10.10.1.0/26)** |
| Boot diagnostics | **Disable** |

* Record the public IP address of **VM2** in the following **VM2 Public IP Address** text box:

**VM2 Public IP Address**  


* Record the name of the new network security group associated to the network interface of **VM2** in the following **VM2 Network Security Group** text box:

**VM2 Network Security Group**  


Expand this hint for guidance on locating the network security group for a virtual machine.

* + Review the documentation on [locating a network security group](https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group" \l "view-all-network-security-groups" \o "Locate a network security group" \t "_blank).

## Check your work

Verify that you have created a virtual machine named VM1.

Verify that you have created a virtual machine named VM2.

# **Verify web connectivity by using network security groups**

* Add an inbound security rule to webNSG 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.

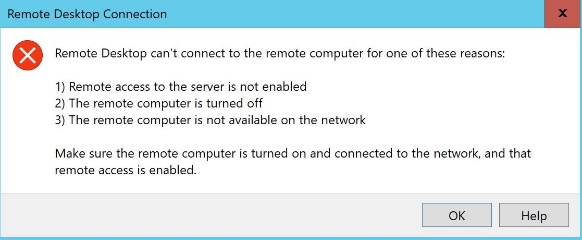
| **Setting** | **Value** |
| --- | --- |
| Destination port ranges | 80,443 |
| Protocol | **TCP** |
| Action | **Allow** |
| Name | AllowAllweb |

* Expand this hint for guidance on creating an inbound security rule.
  + Review the documentation on [creating an inbound security rule](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic" \l "create-security-rules" \o "Create security rules" \t "_blank).
* Attempt to connect to VM1 by using **RDP**.

Expand this hint for guidance on attempting to connect to a virtual machine by using RDP.

* + Review the documentation on attempting to [connect to a virtual machine](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal" \l "connect-to-virtual-machine" \o "Connect to a virtual machine" \t "_blank) by using RDP.

An expected error occurs because the webNSG network security group does not allow RDP traffic from the internet on the web subnet.



* Connect to VM2 by using **RDP** and the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| IP address | **Public IP address (<Admin-PublicIP>)** |
| Username | AzureAdmin |
| Password | Az!26434344! |

* Expand this hint for guidance on connecting to a virtual machine by using RDP.
  + Review the documentation on [connecting to a virtual machine](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal" \l "connect-to-virtual-machine" \o "Connect to virtual machine" \t "_blank) by using RDP.

The connection should be successful because the <Admin-NICNSG> network security group allows RDP traffic from the internet through the network interface on VM2.

* Start **Windows PowerShell**® in the RDP session for **VM2**, and then run the following command to connect to **VM1** by using a nested RDP session:

mstsc /v:VM1

* Sign in as AzureAdmin using Az!26434344! as password.

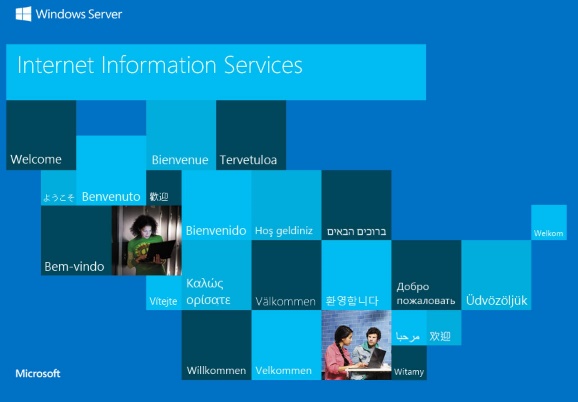
This should connect because, by default, virtual machines in the same virtual network can communicate with each other over any port.

* Install **IIS** in the nested RDP session for **VM1** by using **Windows PowerShell**.

Expand this hint for guidance on installing IIS by using Windows PowerShell.

* + Review the documentation on [installing IIS by using Windows PowerShell](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal" \l "install-web-server" \o "Install web server" \t "_blank).
* Open a new browser window on your local computer, and then go to the IP address of VM1 at http://<Web-PublicIP>.

You should see the default web page for IIS to verify that web traffic has been routed correctly.



## Check your work

Verify that you have created an inbound security rule named AllowAllweb in the webNSG network security group.

Verify that you have created an inbound security rule named RDP in the VM2-nsg network security group.

# **Summary**

Congratulations, you have completed the **Can You Configure Multi-Scope Network Security?** challenge.

In this challenge, you have accomplished the following:

* Created an Azure virtual network that contains subnets and a network security group.
* Deployed an Azure virtual machine to each subnet.
* Verified web connectivity by using network security groups.