

Module 3 - Lab 3 - Filtering Network Traffic with Network Security Groups

? Overview

In this lab, you will create a virtual network, network security groups and an application security group. From there you will associate several security rules and then create several virtual machines associated with them to test filtering network traffic.

Exercise 1: Create a Virtual Network and Security Groups

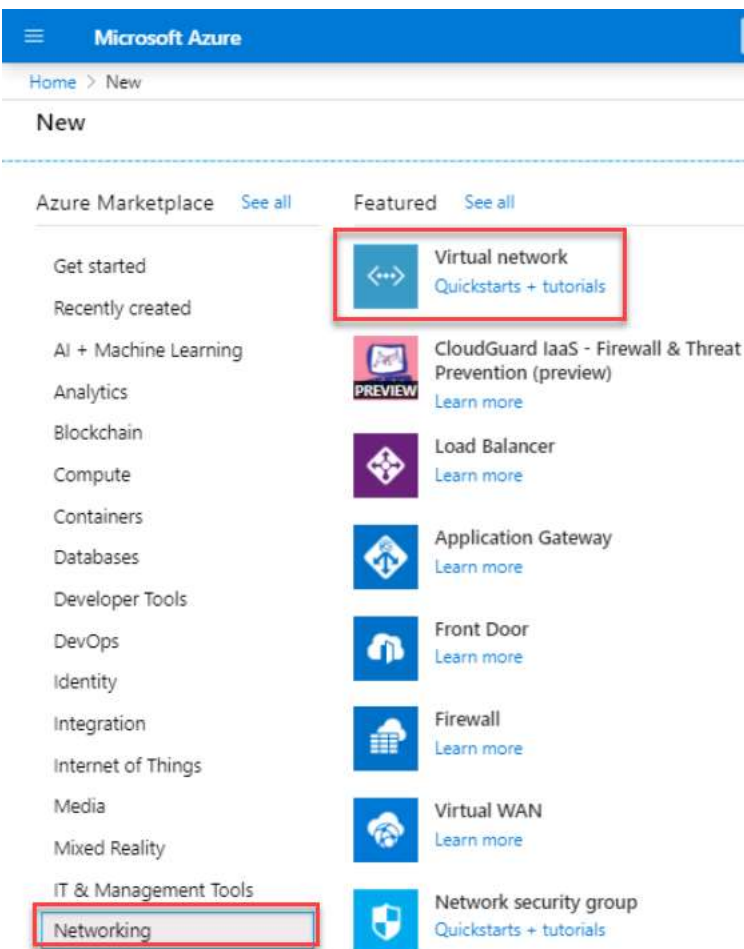
? In this exercise, you will create the lab's virtual network as well as application and network security groups.

Task 1: Create a Virtual Network

- ☐ 1. Launch a browser in the Lab VM and navigate to the URL <https://portal.azure.com> and login with the username sheikhnasirV3ZM@gdcs1.com and password [EvPOwKYcA4jrQ7CO](#)
- ☐ 2. Expand the portal's left navigation by clicking **Show portal menu** in the top left.



- ☐ 3. Click **+ Create a resource > Networking > Virtual Network**



- ☐ 4. In the **Create virtual network** blade, enter the following configuration and click **Next: IP Addresses**.
 - Resource Group: [NSGLabRG-DLPOE1DZAR](#)
 - Name: [NSGLabVN](#)
 - Region: South Central US
- ☐ 5. In The **IP Addresses** tab, enter the following configuration then click **Review + Create** then **Create**.
 - Address Space: [10.0.0.0/16](#)
 - Subnet name: Click **default** then enter **MySubnet** in the **Edit Subnet** blade that appears.

- Subnet Address Range: Enter  10.0.0.0/24 in the **Edit Subnet** blade then click **Save**.

Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16

☐ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet Remove subnet

<input type="checkbox"/> Subnet name	Subnet address range
<input type="checkbox"/> default	10.0.0.0/24

Review + create < Previous Next : Security > Download a template for automation

Edit subnet

Subnet name
MySubnet

Subnet address range
10.0.0.0/24
10.0.0.0 - 10.0.0.255 (256 addresses)

SERVICE ENDPOINT

Create service specific azure service endpoint

Services ⓘ
0 selected

Save



Task 2: Create a Application Security Groups

- ☐ 1. Click + **Create a resource**
- ☐ 2. Search for and select  **Application security group**

Home > New

New

Application security group

- ☐ 3. Click **Create**
- ☐ 4. In the **Create an application security group** blade, enter the following configuration then click **Review + Create** then **Create**.
 - Resource Group:  **NSGLabRG-DLPOE1DZAR**
 - Name:  **myAppSG**
 - Region: **Select the same region you used previously**

Create an application security group

Basics Tags Review + create

Project details

Subscription *

OTA-PRD-887

Resource group *

NSGLabRG

[Create new](#)

Instance details

Name *

myAppSG

Region *

(US) South Central US



Review + create

< Previous

Next : Tags >

[Download a template for automation](#)

- ☐ 5. Repeat steps 1-3 then enter the following configuration. Click **Review + Create** then **Create**.

- Resource Group:  [NSGLabRG-DLPOE1DZAR](#)
- Name:  [myMgmtSG](#)
- Region: **Select the same region as you used previously**

- ☐ 6. This will enable you to group together servers with similar functions.

Task 3: Create a Network Security Group

- ☐ 1. Click + **Create a resource** > **Networking** > **Network security group**

New

 Search the Marketplace

Azure Marketplace [See all](#)

Featured [See all](#)

Get started

Recently created

AI + Machine Learning

Analytics

Blockchain

Compute

Containers

Databases

Developer Tools

DevOps

Identity

Integration

Internet of Things

Media

Mixed Reality

IT & Management Tools

Networking

Software as a Service (SaaS)

Security



Virtual network
[Quickstart tutorial](#)



Check Point CloudGuard IaaS R80.10
Cluster (preview)
[Learn more](#)



Load Balancer
[Learn more](#)



Application Gateway
[Learn more](#)



Front Door
[Learn more](#)



Firewall
[Learn more](#)



Virtual WAN
[Learn more](#)



Network security group
[Quickstart tutorial](#)



ExpressRoute

☐ 2. In the **Create network security group** blade, enter the following configuration then click **Review + Create** then **Create**.

- Resource Group:  **NSGLabRG-DLPOE1DZAR**
- Name:  **_myNSG**
- Location: **Select the same region you used previously**

Create network security group

Basics Tags Review + create

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name * ✓

Region *

Review + create

< Previous

Next : Tags >

[Download a template for automation](#)

✓ **Results:** In this exercise, you successfully created a virtual network along with application security groups and a network security group.

Exercise 2: Associate Network Security Groups to a Subnet and Create Security Rules.

❓ In this exercise, you will associate the network security group created previously to the subnet and then create security rules.

Time Estimate

- 20 minutes

Task 1: Associate the Network Security Group to a Subnet

- ☐ 1. Navigate to your network security group in the portal.
- ☐ 2. Under **Settings**, click **Subnets** Then click + **Associate**.

☐ 3. In the **Associate subnet** blade, enter the following configuration then click **OK**.

- Virtual Network: [NSGLabVN](#)
- Subnet: **MySubnet**

Task 2: Create Security Rules

- ☐ 1. Navigate to your network security group in the portal.
- ☐ 2. Under **Settings**, click **Inbound Security Rules** then click + **Add**

myNSG - Inbound security rules

Network security group

Search (Ctrl+/)

<<

+ Add

Default rules

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces




Subnets


Properties

Locks

Priority	Name	Port	Protocol	Source	Destina...	Action
65000	AllowVnetInBo...	Any	Any	Virtual...	Virtual...	Allow ...
65001	AllowAzureLoa...	Any	Any	AzureL...	Any	Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	Deny ...

3. In the **Add inbound security rule** blade, enter the following configuration then click **Add**.

- Destination: **Application security group**
- Destination application security group:  **myAppSG**
- Destination port ranges:  **80,443**
- Protocol: **TCP**
- Name:  **Allow-Web-All**



Add inbound security rule

myNSG

Basic

Source * ⓘ

Any

Source port ranges * ⓘ

*

Destination * ⓘ

Application security group

Destination application security group * ⓘ

myAppSG

Destination port ranges * ⓘ

80,443

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

100




Name *


Allow-Web-All


Description

Add

4. Click + **Add** again, then enter the following configuration and click **Add**.

- Destination: **Application security group**
- Destination application security group:  **myMgmtSG**
- Destination port ranges:  **3389**
- Protocol: **TCP**
- Name:  **Allow-RDP-All**

 **Add inbound security rule**
myNSG

 Basic

Source * ⓘ

Any

Source port ranges * ⓘ

*

Destination * ⓘ

Application security group

Destination application security group * ⓘ

myMgmtSG

Destination port ranges * ⓘ

3389

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority * ⓘ

110

Name *

Allow-RDP-All

Description

Add

✓ **Results:** In this exercise, you successfully associated the network security group to the subnet and created security rules.

Exercise 3: Configuring and Testing Traffic Filters

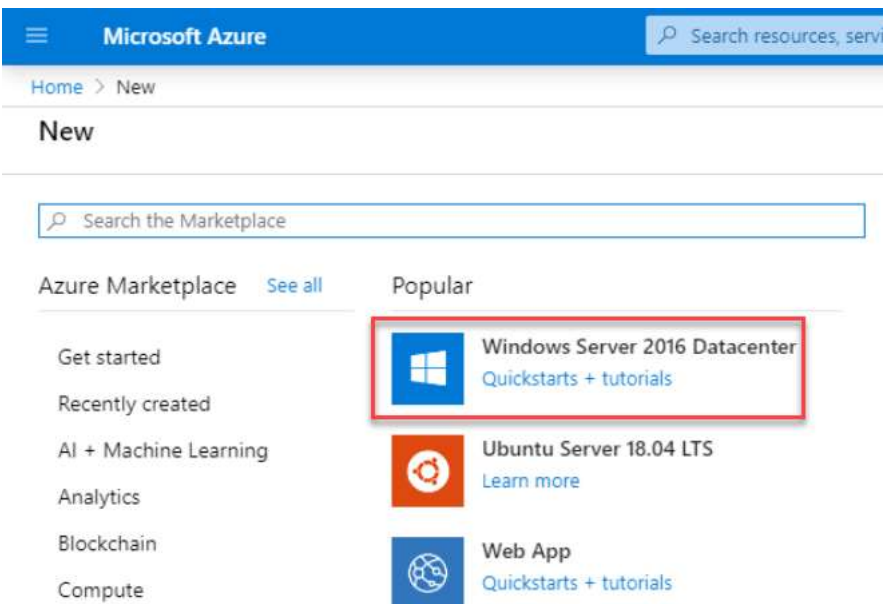
❓ In this exercise, you will create two virtual machines in the virtual network. Then you will add each virtual machine's network interface to the application security groups created earlier. Finally, you will test the traffic filters.

Time Estimate

- 30 minutes

Task 1: Create Virtual Machines

1. Click + **Create a Resource** search for and select **Windows Server 2016 Datacenter**



- ☐ 2. In the **Create a virtual machine** blade, enter the following configuration then click **Next: Disks** then **Next: Networking**.

- Resource Group: **NSGLabRG-DLPOE1DZAR**
- Name: **VMWeb**
- Region: **Select the same region you've been using**
- Size: **Standard D2S_V3**
- Username: **localadmin**
- Password/Confirm Password: **EvPOwKYcA4jrQ7CO**

Create a virtual machine

⚠ Changing Basic options may reset selections you have made. Review all options prior to creating the virtual machine.

Basics | Disks | Networking | Management | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for classic VMs? [Create VM from Azure Marketplace](#)

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Opogility Development Environment

Resource group * **NSGLabRG** [Create new](#)

Instance details

Virtual machine name * **VMWeb**

Region * **(US) North Central US**

Availability options No infrastructure redundancy required

Image * Windows Server 2016 Datacenter [Browse all public and private images](#)

Size * **Standard D2s v3**
2 vcpus, 8 GiB memory [Change size](#)

- ☐ 3. On the **Networking** section, enter the following configuration then click **Review + Create** then **Create**.

- Virtual Network: **NSGLabVN**
- NIC Network Security Group: **Advanced**
- Configure Network Security Group: **myNSG**

Create a virtual machine

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ **NSGLabVN** Create new

Subnet * ⓘ **MySubnet (10.0.0.0/24)** Manage subnet configuration

Public IP ⓘ **(new) VMWeb-ip** Create new

NIC network security group ⓘ ☐ None ☐ Basic ☒ **Advanced**

Configure network security group * **myNSG** Create new

Accelerated networking ⓘ ☐ On ☒ Off The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? ☐ Yes ☒ No

Review + create < Previous Next : Management >

- ☐ 4. Repeat Steps 1-3 except name the VM **VMgmt**.
- ☐ 5. Wait for the VMs to be fully deployed before moving to the next task.

Task 2: Associate network interfaces to ASGs

- ☐ 1. Navigate to the **VMWeb** VM.
- ☐ 2. Under **Settings** select **Networking** then click **Application security groups** then **Configure the application security groups**

VMWeb - Networking
Virtual machine

Search (Ctrl+/)

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings

Networking Disks

Attach network interface Detach network interface

Network interface: vmweb961 Effective security rules Topology

Virtual network/subnet: NSGLabVN/MySubnet NIC Public IP: 52.162.210.13 NIC Private IP: 10.0.0.4 Accelerated networking: Disabled

Inbound port rules Outbound port rules **Application security groups** Load balancing

Configure the application security groups

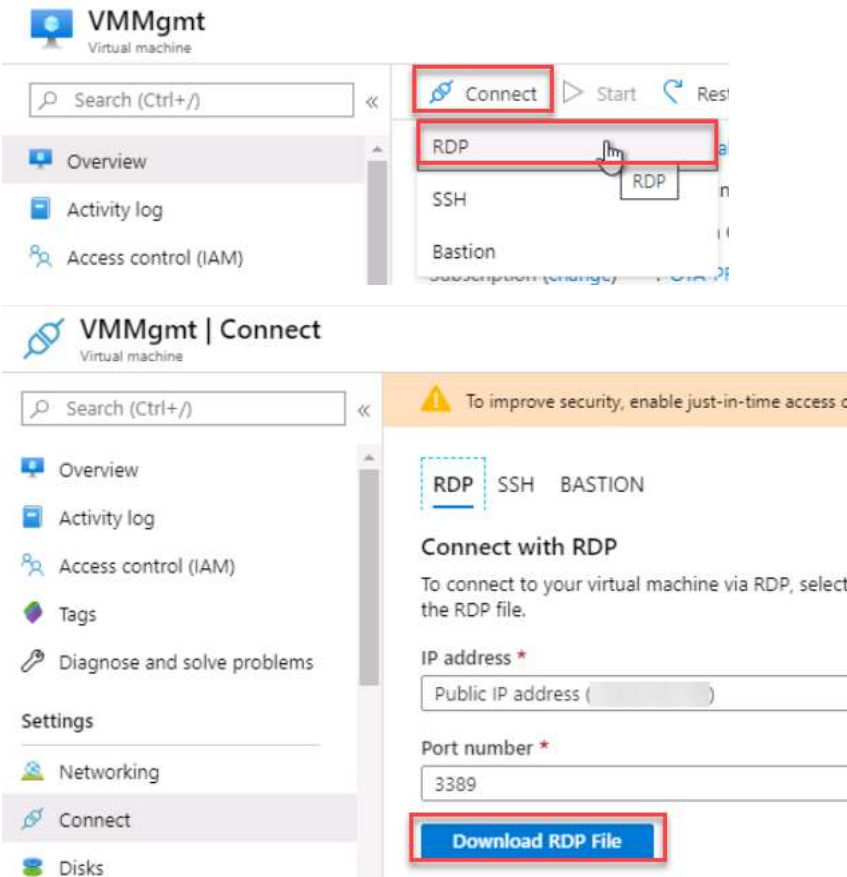
- ☐ 3. In the **Configure application security groups** blade, select **myAppSG** from the dropdown then click **Save**.



- ☐ 4. Repeat steps 1-3 for the **VMMgmt** VM except choose the **myMgmtSG** ASG.

Task 3: Test the Traffic Filters

- ☐ 1. Navigate to the **VMMgmt** VM.
- ☐ 2. Click **Connect** then **RDP**. Then click **Download RDP File**.



- ☐ 3. Click **Connect** then enter the VM's credentials. Click **Yes** at the next prompt.

- Username: **localadmin**
- Password: **EvPOwKYcA4jrQ7CO**

- ☐ 4. Open **PowerShell** from the Start menu then enter the following command.

```
mstsc /v:VMWeb
```

- ☐ 5. Enter the credentials for **VMWeb** and then click **Yes** at the prompt.

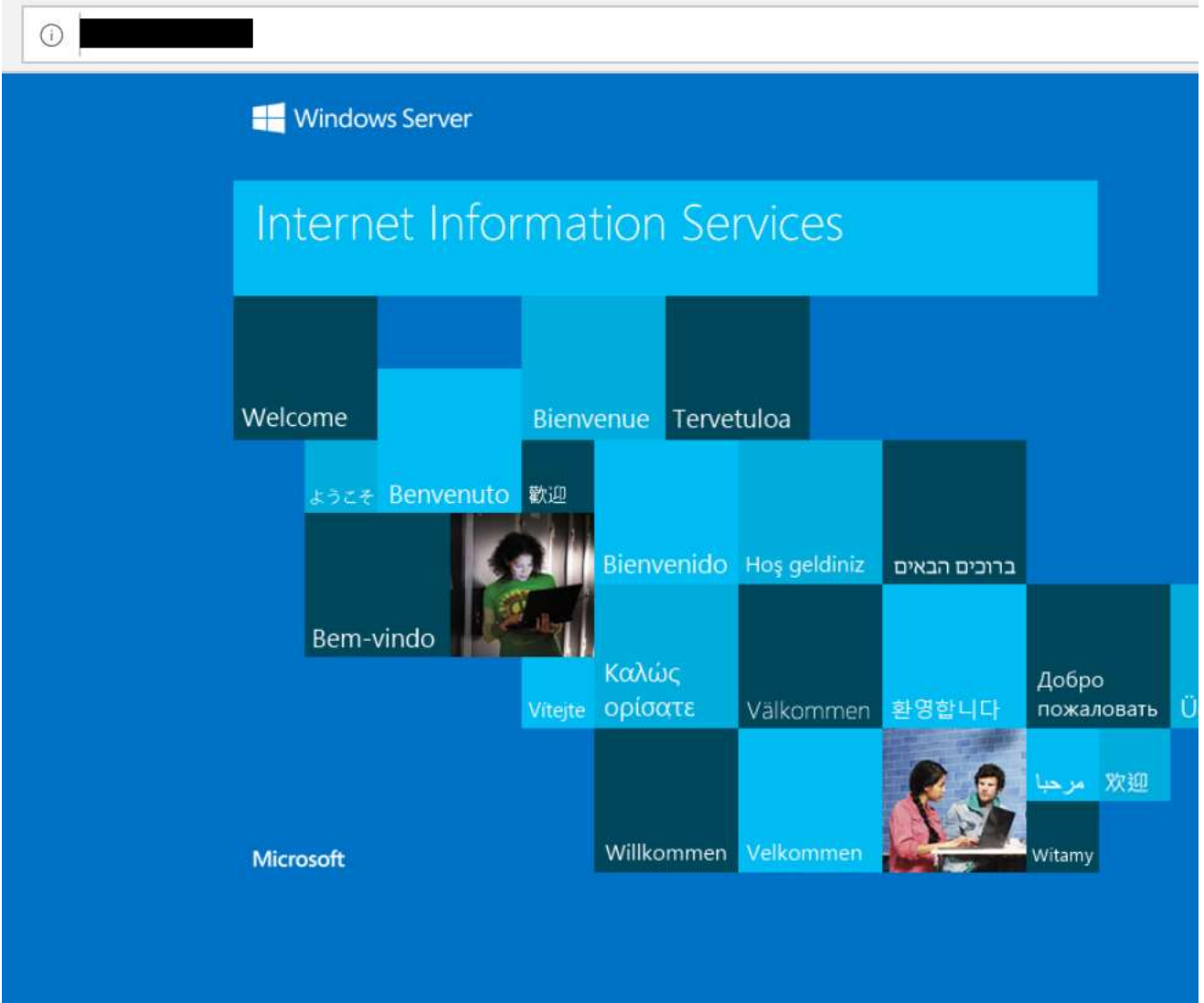
- Username: **localadmin**
- Password: **EvPOwKYcA4jrQ7CO**

- ☐ 6. You are able to connect to the **VMWeb** VM from the **VMMgmt** VM because the VMs are in the same virtual network. However, you cannot create a remote desktop connection to the **VMWeb** VM from the internet, because the security rule created earlier doesn't allow inbound traffic from the Internet on port 3389 and inbound traffic from the Internet is denied to all resources by default.

- ☐ 7. Open PowerShell on **VMWeb** and install Microsoft IIS using the following command

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

- ☐ 8. Once the installation completes, disconnect from both RDP sessions by clicking the 'X' icon in the top blue bar.



- ☐ 9. Navigate to the **VMWeb** VM in the portal.
- ☐ 10. Copy the public ip address then navigate to it in a new browser tab.
- ☐ 11. You see the IIS welcome screen. This is because inbound traffic from the Internet is allowed on port 80 to the **myAppSG** application security group that the network interface attached to the **VMWeb** VM is in.

✓ **Results:** In this exercise, you created two virtual machines in the virtual network. You then added each virtual machine's network interface to the application security groups created earlier. Finally, you tested the traffic filters.