



Microsoft Cloud Workshop

Enterprise-class networking in Azure

Hands-on lab step-by-step

November 2017

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2017 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners

Contents

Enterprise-class networking in Azure hands-on lab step-by-step	1
Abstract and learning objectives	1
Overview	1
Requirements	2
Help References	2
Before the hands-on lab	4
Task 1: Create a virtual machine to execute the lab in	4
Task 2: Update Azure PowerShell version	10
Task 3: Download hands-on lab step-by-step support files	13
Exercise 1: Create a virtual network and provision subnets	14
Task 1: Create a virtual network	14
Task 2: Configure subnets	15
Exercise 2: Create route tables with required routes	19
Task 1: Create route tables	19
Task 2: Add routes to each route table	21
Exercise 3: Deploy n-tier application and validate functionality	28
Task 1: Use the Azure portal for a template deployment	28
Task 3: Validate the CloudShop application is up after the deployment	30
Task 4: Create a load balancer to distribute load between the web servers	33
Task 5: Configure the load balancer	34
Exercise 4: Build the management station	40
Task 1: Build the management VM	40
Exercise 5: Provision and configure partner firewall solution	46
Task 1: Removing a spending cap and associating a credit card with your subscription	46
Task 2: Provision the firewall appliance	48
Task 3: Enable IP forwarding on the firewall network interface	52
Exercise 6: Configure the firewall to control traffic flow	55
Task 1: Log on to pfSense and add aliases	55
Task 2: Add NAT rules	58
Task 3: Configure firewall rules	63
Task 4: Associate route tables to subnets	71
Task 5: Validate connectivity	74
RDP to WGMGMT1 server and from MGMT to WEB server	74
Validate internal connectivity to CloudShop	75
Exercise 7: Configure site-to-site connectivity	78
Task 1: Create another virtual network	78
Task 2: Configure gateway subnets for both virtual networks	79

Task 3: Create the first gateway	82
Task 4: Create the second gateway.....	84
Task 5: Connect the gateways.....	87
Exercise 8: Validate connectivity from 'on-premises' to Azure	91
Task 1: Create a virtual machine to validate connectivity	91
Task 2: Configure routing for simulated 'on-premises' to Azure traffic	92
Task 3: Add a firewall rule on pfSense	95
Task 4: Validate connectivity from 'on-prem' to 'Azure' side	96
After the hands-on lab	100

Enterprise-class networking in Azure hands-on lab step-by-step

Abstract and learning objectives

In this workshop, students will learn how to setup and configure a Virtual Network with Subnets in Azure. Students will also learn how to secure the Virtual Network with Firewall rules and route tables. Additionally, students will set up access to the Virtual Network with a "jump box" and a site-to-site VPN connection.

Attendees will be better able to plan and design virtual networks in Azure with multiple subnets to filter and control network traffic. In addition,

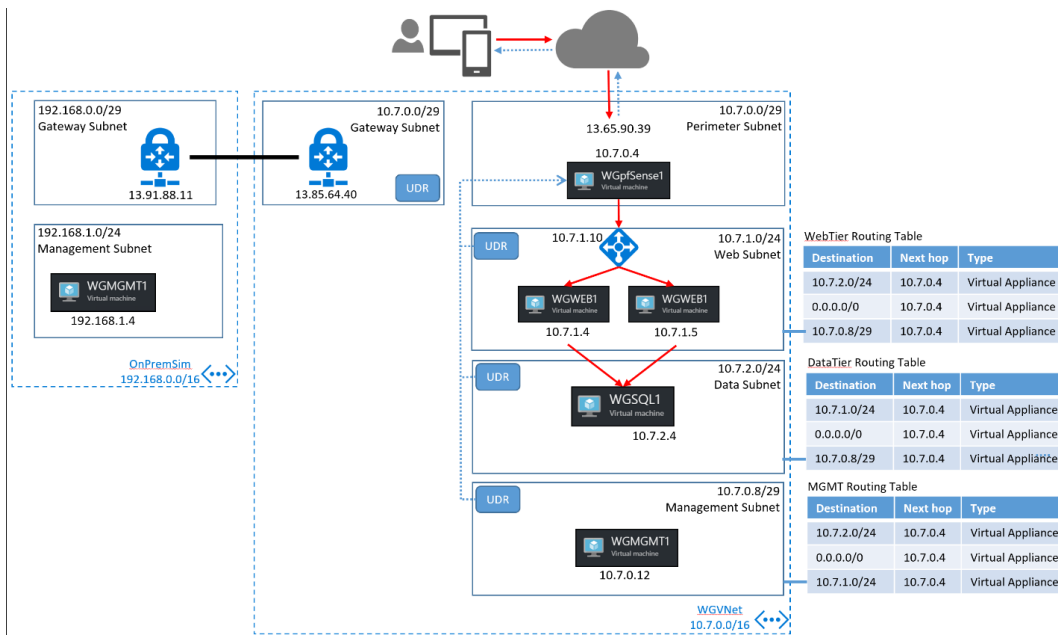
- Create a Virtual Network and provision subnets
- Create route tables with required routes
- Build a management "jump box"
- Configure firewall to control traffic flow
- Configure site-to-site connectivity

Overview

You have been asked by Woodgrove Financial Services to provision a proof of concept deployment that will be used by the Woodgrove team to gain familiarity with a complex virtual networking deployment, including all of the components that enable the solution. Specifically, the Woodgrove team will be learning about:

- How to bypass system routing to accomplish custom routing scenarios
- How to capitalize on load balancers to distribute load and ensure service availability
- How to implement a partner firewall solution to control traffic flow based on policies.

The result of this proof of concept will be an environment resembling this diagram:



Requirements

You must have a working Azure subscription to carry out this hands-on lab step-by-step without a spending cap to deploy the pfSense firewall from the Azure Marketplace.

Help References

Description	Links
IP Addressing and Subnetting for New Users	http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html
CIDR / VLSM Supernet Calculator	http://www.subnet-calculator.com/cidr.php
Virtual Network documentation	https://azure.microsoft.com/en-us/documentation/services/virtual-network/
Network Security Group documentation	https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/
IP addresses in Azure	https://azure.microsoft.com/en-us/documentation/articles/virtual-network-ip-addresses-overview-arm/
User-Defined Routing and IP Forwarding	https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-udr-overview/
Load Balancer	https://azure.microsoft.com/en-us/documentation/articles/load-balancer-overview/
Implementing a DMZ between Azure and your on-premises datacenter	https://azure.microsoft.com/en-us/documentation/articles/guidance-iaas-ra-secure-vnet-hybrid/

Description	Links
pfSense firewall rule basics	https://doc.pfsense.org/index.php/Firewall Rule Basics
How can I forward ports with pfSense	https://doc.pfsense.org/index.php/How can I forward ports with pfSense

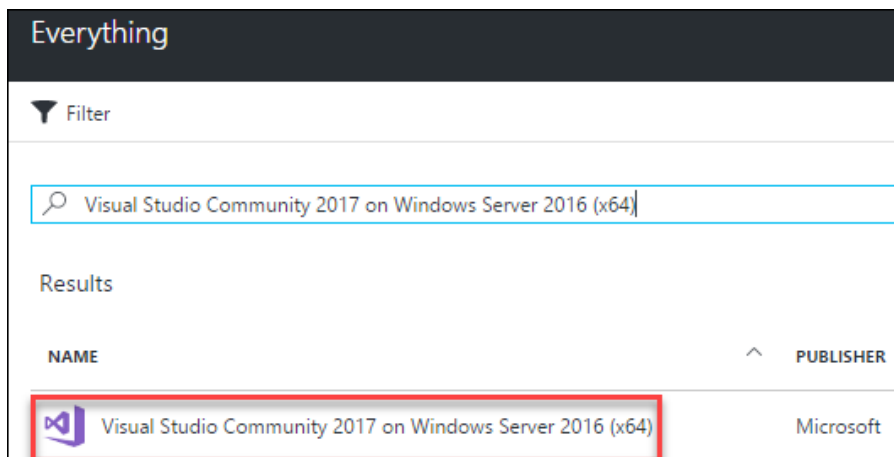
Before the hands-on lab

Duration: 15 minutes

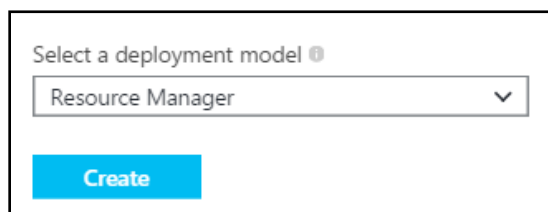
If you are working on a machine that cannot run PowerShell, carry out this task. Only do this if you are not running the commands on your local machine and are provisioning a VM to perform the steps.

Task 1: Create a virtual machine to execute the lab in

1. Launch a browser, and navigate to <https://portal.azure.com>. Once prompted, login with your Microsoft Azure credentials. If asked, choose whether your account is an organization account or just a Microsoft Account.
2. Click on **+NEW**, and in the search box, type in **Visual Studio Community 2017 on Windows Server 2016 (x64)**, and press enter. Click the Visual Studio Community 2017 image running on Windows Server 2016 with the latest update.
3. In the returned search results, click the image name.



4. In the Marketplace solution blade, at the bottom of the page keep the deployment model set to **Resource Manager**, and click **Create**.



5. Set the following configuration on the Basics tab, and click **OK**.
 - Name: **LABVM**
 - VM disk type: **SSD**

- User name: **demouser**
- Password: **demo@pass123**
- Subscription: **If you have multiple subscriptions, choose the subscription to execute your labs in.**
- Resource Group: **OPSLABRG**
- Location: **Choose the closest Azure region to you.**

The screenshot shows the 'Basics' configuration window for an Azure VM. The fields are as follows:

- Name:** LABVM (checked)
- VM disk type:** SSD
- User name:** demouser
- Password:** (masked)
- Confirm password:** (masked)
- Subscription:** (dropdown menu)
- Resource group:** Create new (selected), OPSLABRG (checked)
- Location:** South Central US

6. Choose the **DS1_V2 Standard** or **F2S** instance size on the Size blade.

Note: You may have to click the View All link to see the instance sizes.

Choose a size
Browse the available sizes and their features

Prices presented are estimates in your local currency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Recommended sizes are determined by the publisher of the selected image based on hardware and software requirements.

★ Recommended | View all

DS1_V2 Standard	DS2_V2 Standard ★	DS3_V2 Standard
1 Core	2 Cores	4 Cores
3.5 GB	7 GB	14 GB
2 Data disks	4 Data disks	8 Data disks
3200 Max IOPS	6400 Max IOPS	12800 Max IOPS
7 GB Local SSD	14 GB Local SSD	28 GB Local SSD
Load balancing	Load balancing	Load balancing
Premium disk support	Premium disk support	Premium disk support
47.62 USD/MONTH (ESTIMATED)	94.49 USD/MONTH (ESTIMATED)	189.72 USD/MONTH (ESTIMATED)

Note: If the Azure Subscription you are using is NOT a trial Azure subscription, you may want to choose the DS2_V2 to have more power in this LABMV. If you are using a Trial Subscription or one that you know has a restriction on the number of cores, stick with the DS1_V2.

7. Click **Configure required settings** to specify a storage account for your virtual machine if a storage account name is not automatically selected for you.

Settings

Storage

Use managed disks ⓘ

No Yes

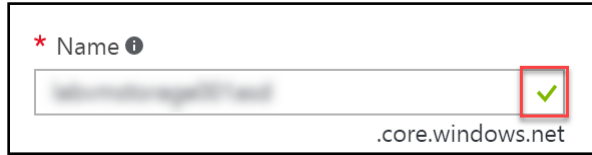
* Storage account ⓘ

Configure required settings >

8. Click **Create New**.

+ Create new

- Specify a unique name for the storage account (all lower letters and alphanumeric characters), and ensure the green checkmark shows the name is valid.

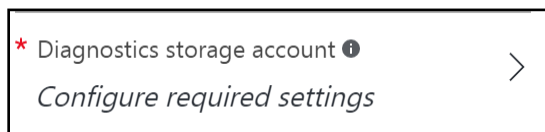


A screenshot of a form field for a storage account name. The field is labeled "* Name" with an information icon. The text "storageaccountname" is entered, followed by ".core.windows.net". A green checkmark is visible in a small box on the right side of the input field, indicating the name is valid.

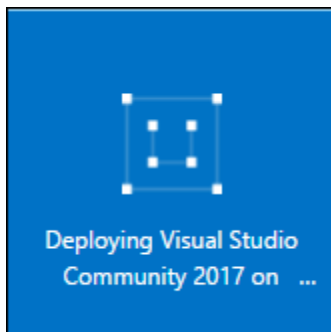
- Click **OK** to continue.



- Click **Configure required settings** for the Diagnostics storage account if a storage account name is not automatically selected for you. Repeat the previous steps to select a unique storage account name. This storage account will hold diagnostic logs about your virtual machine that you can use for troubleshooting purposes.



- Accept the remaining default values on the Settings blade, and click **OK**. On the Summary page, click **OK**. The deployment should begin provisioning. It may take 10+ minutes for the virtual machine to complete provisioning.

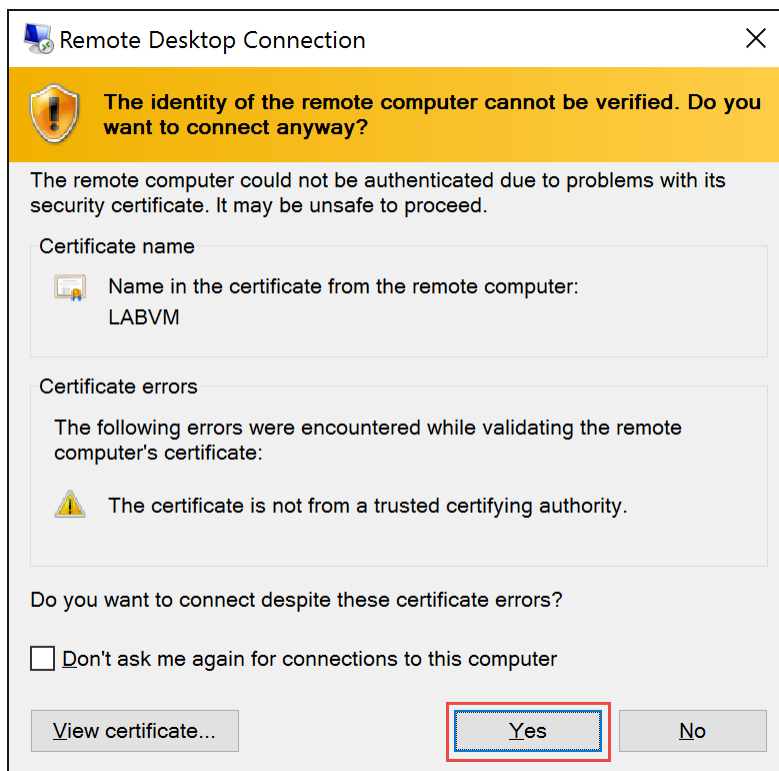


NOTE: Please wait for the LABVM to be provisioned prior to moving to the next step.

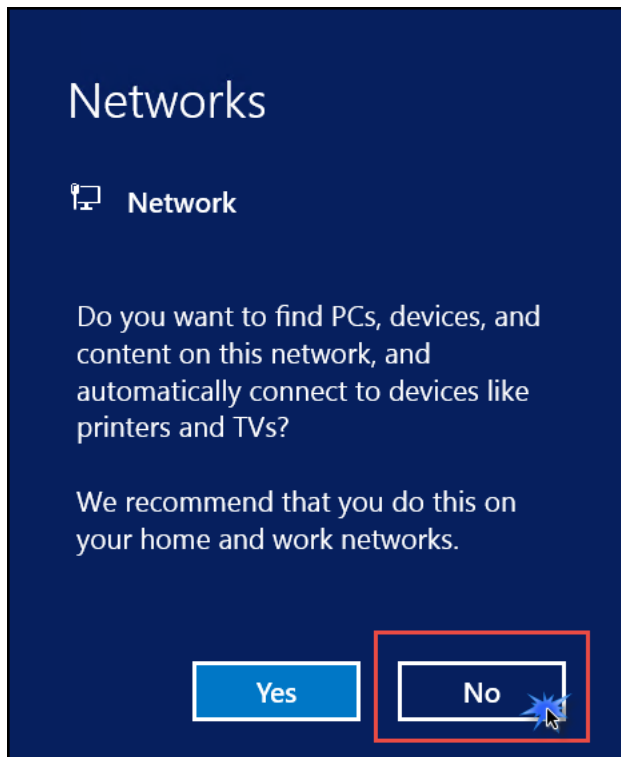
- Move back to the Portal page on your local machine, and wait for **LABVM** to show the Status of **Running**. Click **Connect** to establish a new Remote Desktop Session.



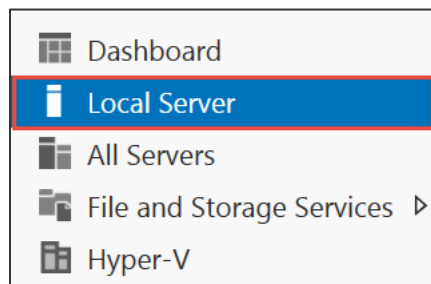
14. Depending on your Remote Desktop protocol client and browser configuration, you will either be prompted to open an RDP file, or you will need to download it and then open it separately to connect.
15. Log in with the credentials specified during creation:
 - a. User: **demouser**
 - b. Password: **demo@pass123**
16. You will be presented with a Remote Desktop Connection warning because of a certificate trust issue. Click **Yes** to continue with the connection.



17. When logging on for the first time, you will see a prompt on the right asking about network discovery. Click **No**.



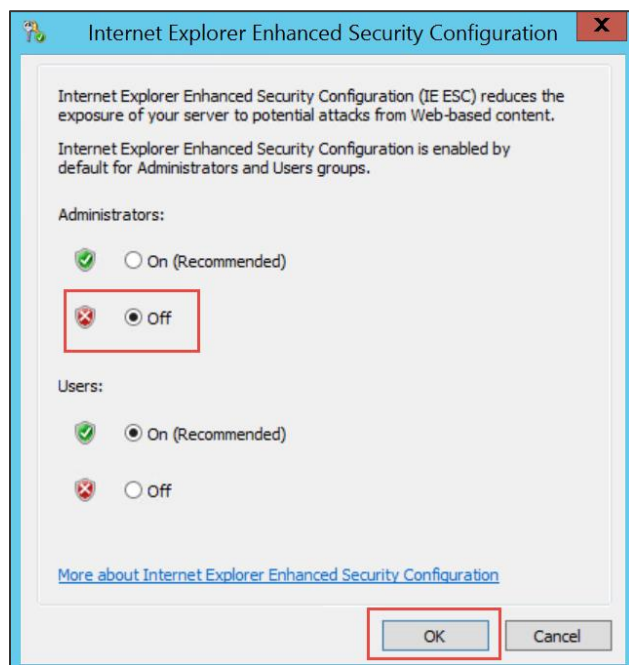
18. Notice that Server Manager opens by default. On the left, click **Local Server**.



19. On the right side of the pane, click **On** by **IE Enhanced Security Configuration**.

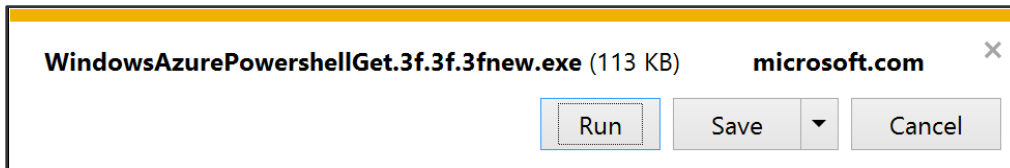
Last installed updates	Never
Windows Update	Install updates automatically using Windows Update
Last checked for updates	Never
Windows Error Reporting	Off
Customer Experience Improvement Program	Not participating
IE Enhanced Security Configuration	On
Time zone	(UTC) Coordinated Universal Time
Product ID	00253-50000-00000-AA006 (activated)
Processors	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz
Installed memory (RAM)	3.5 GB
Total disk space	177 GB

20. Change to **Off** for Administrators, and click **OK**.

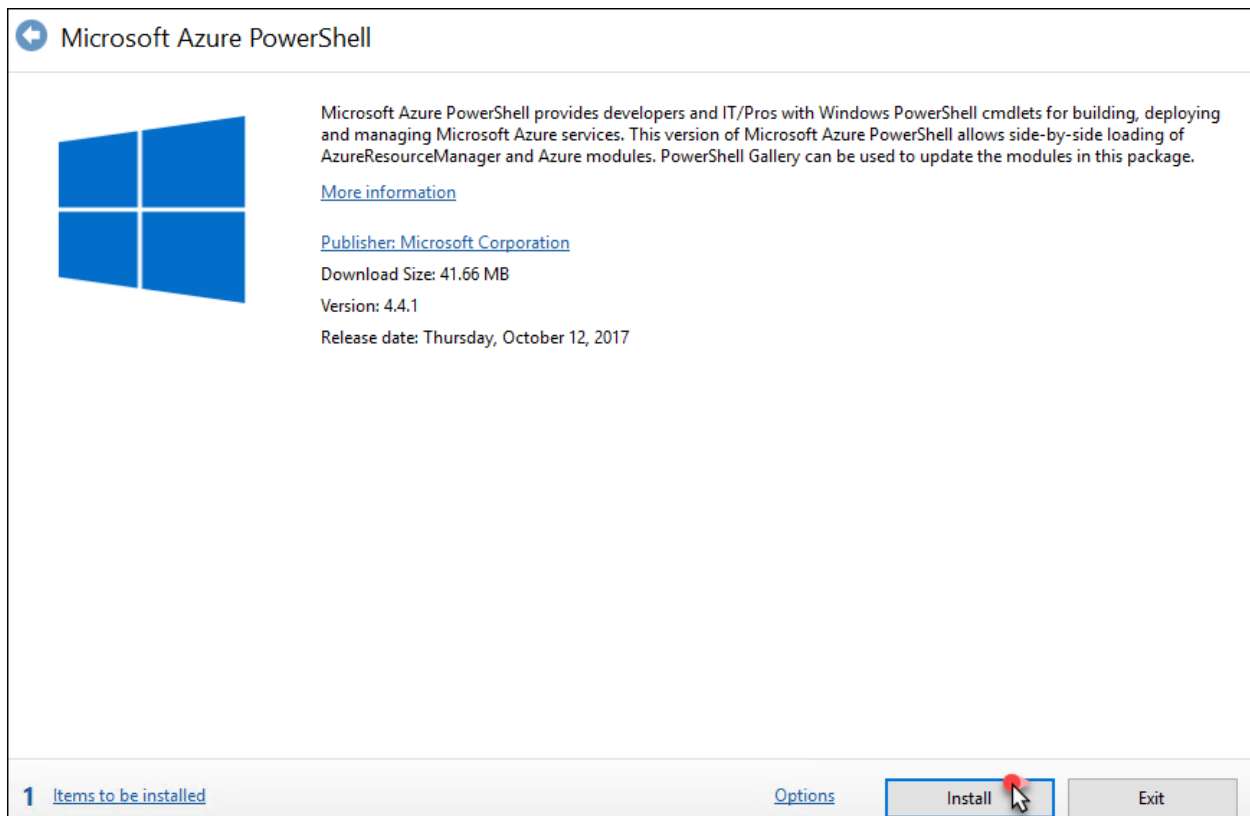


Task 2: Update Azure PowerShell version

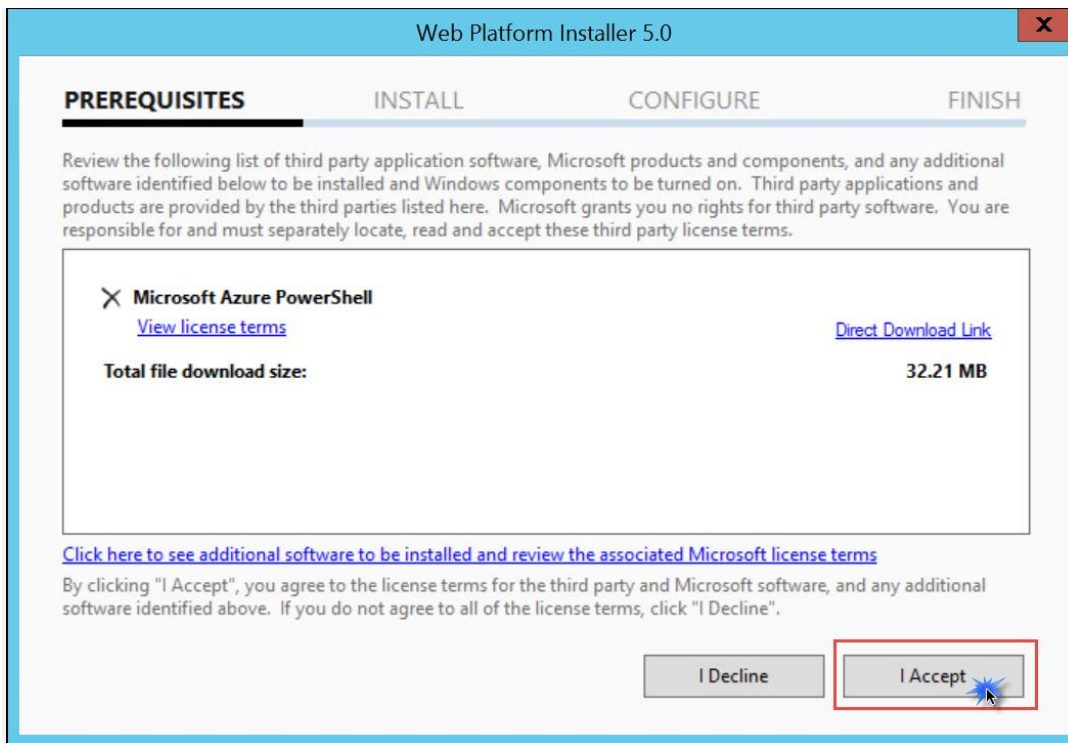
1. While logged into **LABVM** via Remote Desktop, open Internet Explorer, and navigate to <http://aka.ms/webpi-azps>. This will download an executable. After the download is finished, click **Run** to execute it.



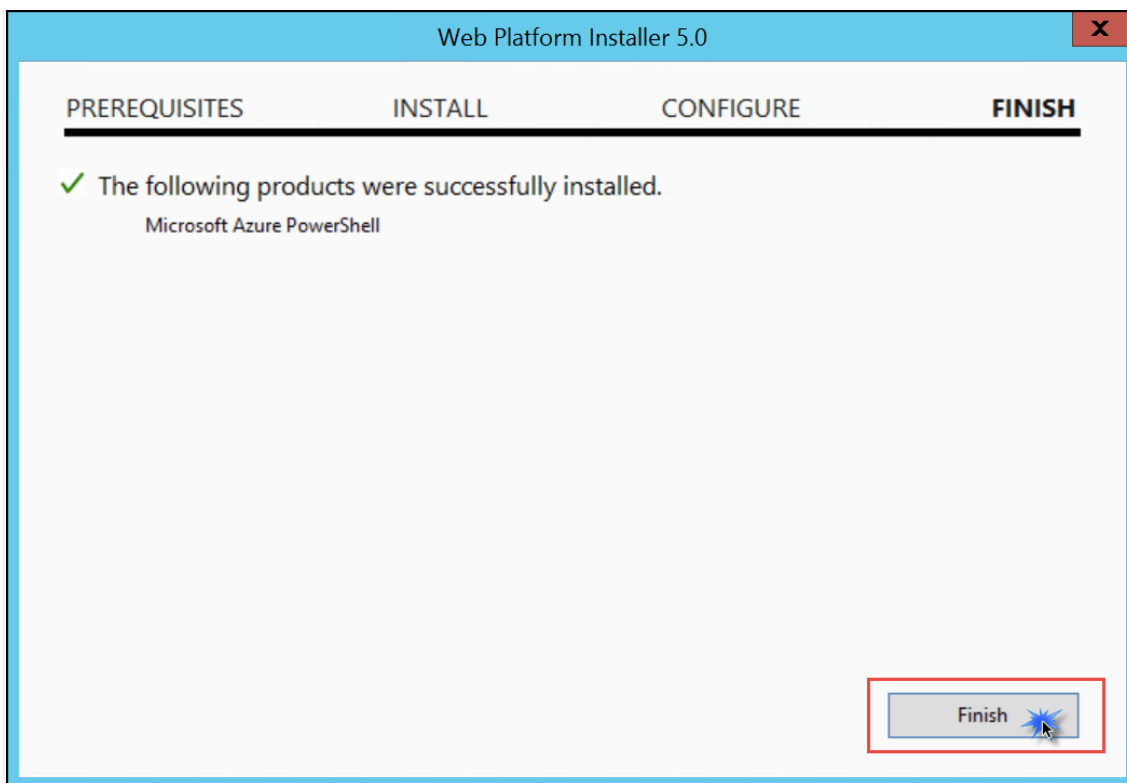
2. A Web Platform Installer dialog box will open. Click **Install** to install the latest version of the Azure PowerShell module (your version may differ from the screenshot). Note: the version on the virtual machine may already be up-to-date.



3. Accept the license terms by clicking **I Accept**.



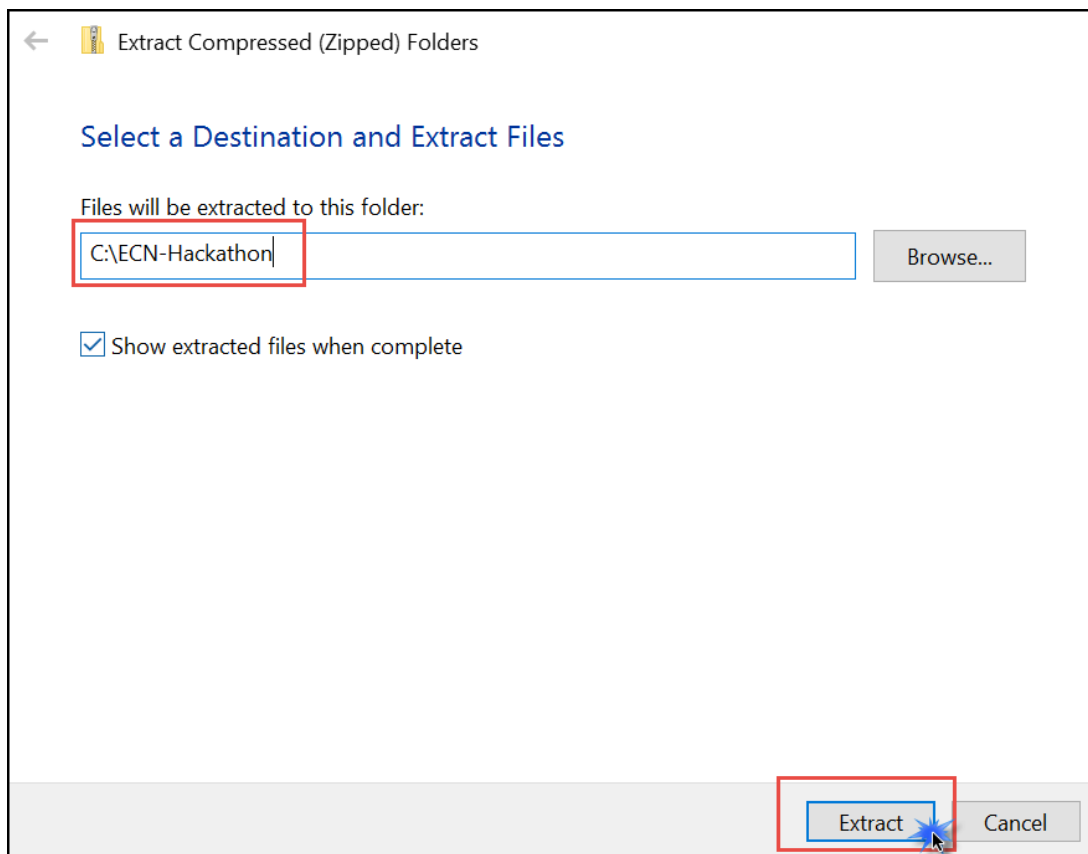
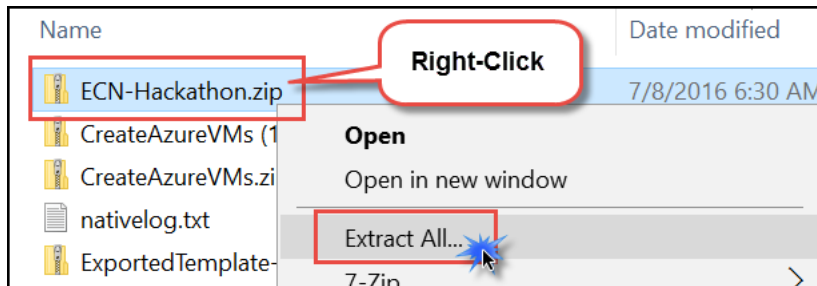
4. Click **Finish** to complete the installation.



5. After the installation is complete, **reboot** the machine you installed Azure PowerShell on.

Task 3: Download hands-on lab step-by-step support files

1. After the reboot has completed, download the zipped hands-on lab step-by-step student files by clicking on this link: <https://cloudworkshop.blob.core.windows.net/enterprise-networking/ECN-Hackathon.zip>
2. Extract the downloaded files into the directory **C:\ECN-Hackathon**.

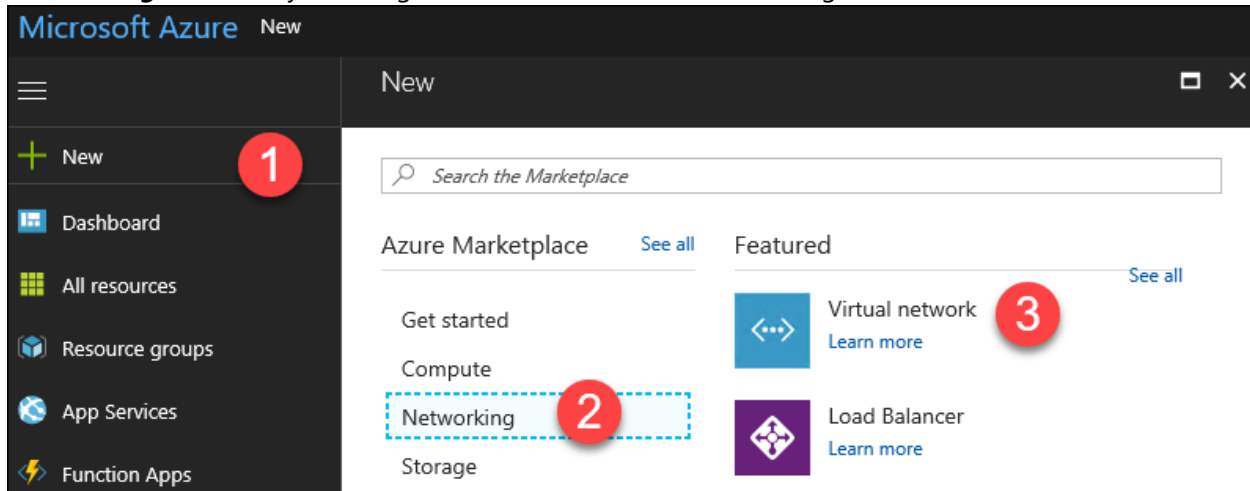


Exercise 1: Create a virtual network and provision subnets

Duration: 15 minutes

Task 1: Create a virtual network

1. From your **LABVM**, connect to the Azure portal, click on **New**, and in the list of Marketplace categories, click **Networking** followed by selecting **Virtual Network**. See the following screenshot for more details.



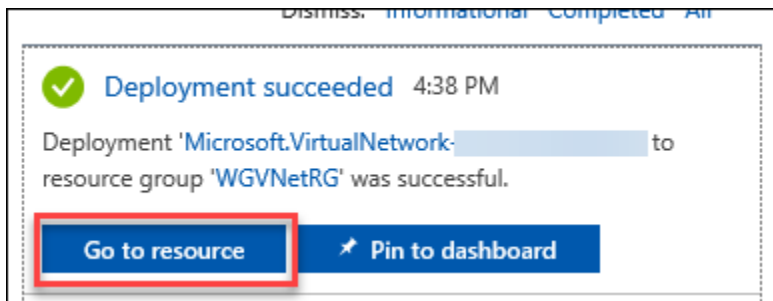
2. On the **Create virtual network** blade, enter the following information:
 - a. Name: **WGVNet**
 - b. Address space: **10.7.0.0/16**
 - c. Subscription: **Choose your subscription**
 - d. Resource group: Select **Create new**, and enter the name **WGVNetRG**
 - e. Location: **West US**
 - f. Subnet name: **Perimeter**
 - g. Subnet address range: **10.7.0.0/29**

Upon completion, it should look like the following screenshot. Validate the information is correct and click **Create**.

Create virtual network

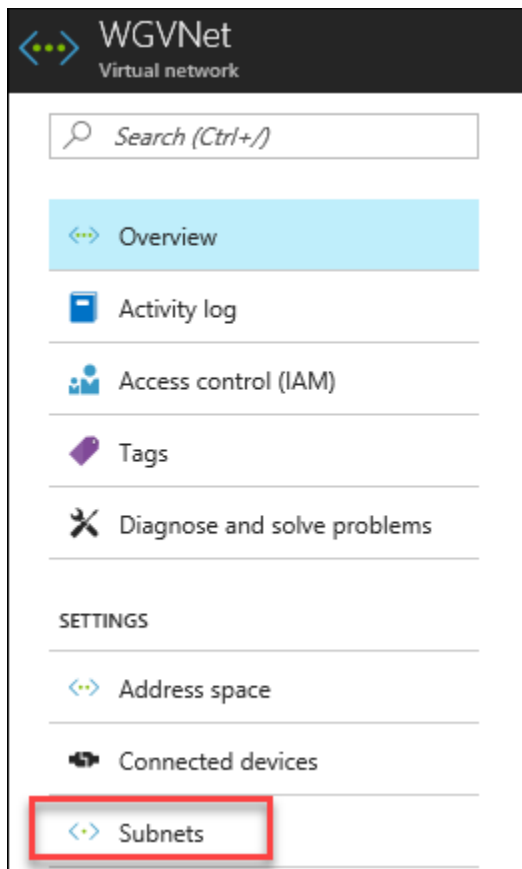
- * Name: WGVNet ✓
- * Address space ⓘ: 10.7.0.0/16 ✓
10.7.0.0 - 10.7.255.255 (65536 addresses)
- * Subscription: [Dropdown]
- * Resource group:
 - Create new
 - Use existing
 WGVNetRG ✓
- * Location: West US ✓
- Subnet
 - * Name: Perimeter ✓
 - * Address range ⓘ: 10.7.0.0/29 ✓
10.7.0.0 - 10.7.0.7 (8 addresses)

3. Monitor the deployment status by clicking on the **Notifications** button in the portal. In a minute or so, you should see a confirmation of the successful deployment. Click the **Go to Resource** button.

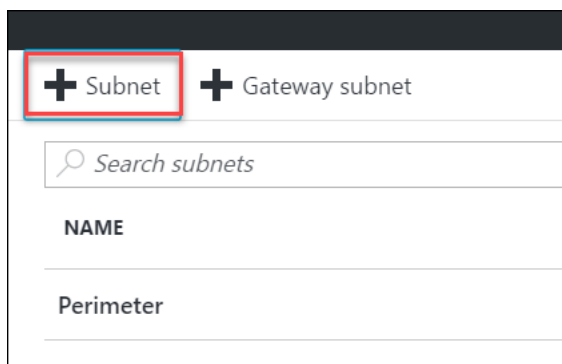


Task 2: Configure subnets

1. Select **WGVNet** blade, and click **Subnets**.



2. In the **Subnets** blade click on **+Subnet**.



3. On the **Add subnet** blade, enter the following information:
 - a. Name: **Management**
 - b. Address range: **10.7.0.8/29**
 - c. Network security group: **None**
 - d. Route table: **None**

When your dialog looks like the following screenshot, click **OK** to create the subnet.

Add subnet
WGVNet

* Name
Management ✓

* Address range (CIDR block) ⓘ
10.7.0.8/29
10.7.1.0 - 10.7.1.255 (256 addresses)

Network security group
None >

Route table
None >

OK

4. Repeat steps 8 and 9 to create the **WebTier** subnet.
 - a. Name: **WebTier**
 - b. Address range: **10.7.1.0/24**
 - c. Network security group: **None**
 - d. Route table: **None**
5. Repeat steps 8 and 9 to create the **DataTier** subnet.
 - a. Name: **DataTier**
 - b. Address range: **10.7.2.0/24**
 - c. Network security group: **None**
 - d. Route table: **None**

The result should look like the following screenshot:

The screenshot shows the Azure portal interface for a virtual network named 'WGVNet'. The left-hand navigation pane includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and a SETTINGS section with Address space, Connected devices, and Subnets (which is highlighted). The main content area shows a '+ Subnet' and '+ Gateway subnet' button, a search bar for subnets, and a table listing the subnets.

NAME	ADDRESS RANGE	AVAILABLE ADDRESSES
Perimeter	10.7.0.0/29	3
Management	10.7.0.8/29	3
WebTier	10.7.1.0/24	251
DataTier	10.7.2.0/24	251

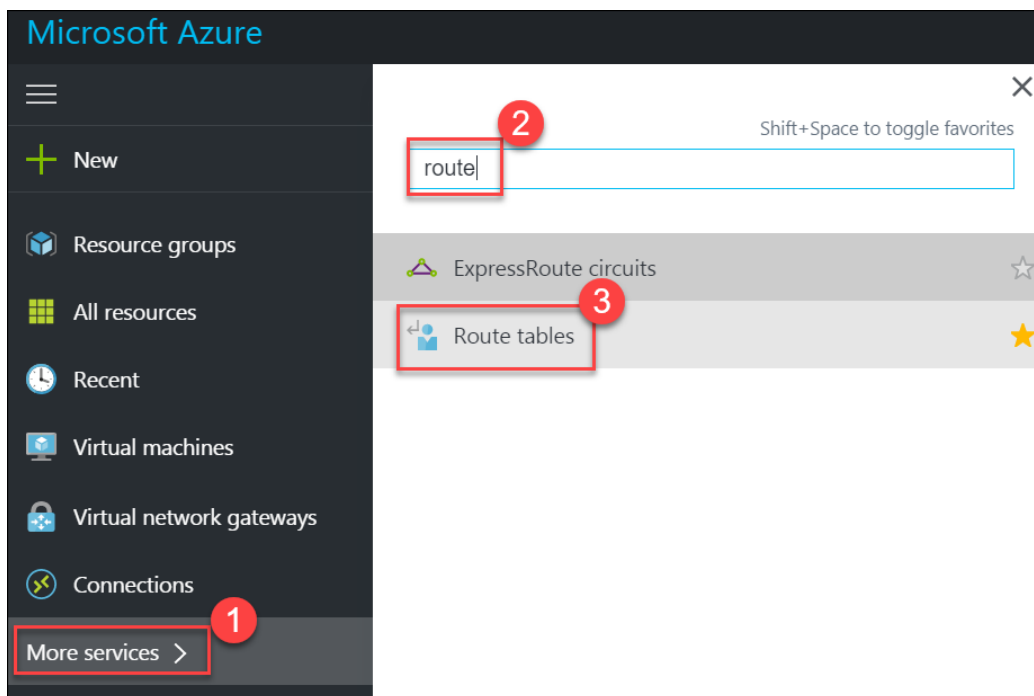
Exercise 2: Create route tables with required routes

Duration: 15 minutes

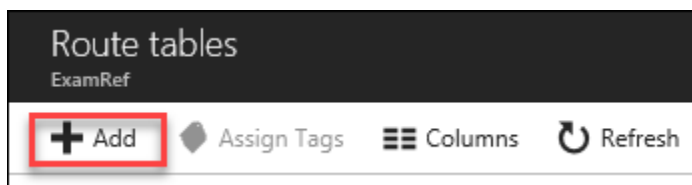
Route Tables are containers for User Defined Routes (UDRs). The route table is created and associated with a subnet. UDRs allow you to direct traffic in ways other than normal system routes would. In this case, UDRs will direct traffic from 'internal' subnets to the firewall appliance.

Task 1: Create route tables

1. On the main portal menu to the left, click **More services** located at the bottom of the menu. Type **route** into the search box, and click on **Route tables**.

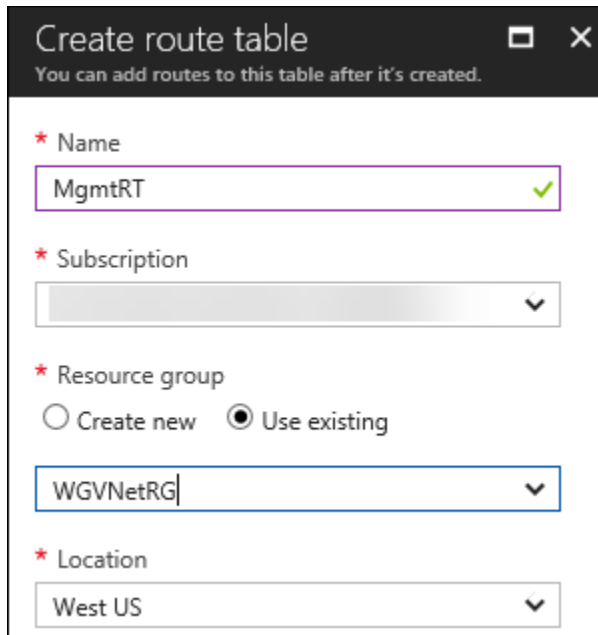


2. On the **Route tables** blade, click **Add**.



3. On the **Route table** blade enter the following information:
 - a. Name: **MgmtRT**
 - b. Subscription: **Choose your subscription**
 - c. Resource group: Select **Use existing**, click the drop-down menu, and select **WGVNetRG**
 - d. Location: **West US**

When the dialog looks like the following screenshot, click **Create**.



Create route table
You can add routes to this table after it's created.

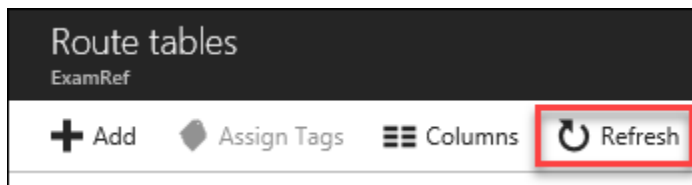
* Name
MgmtRT ✓

* Subscription
▼

* Resource group
 Create new Use existing
WGVNetRG ▼

* Location
West US ▼

4. After a few seconds, if the new route table does not show in the portal, click **Refresh**.



5. After you see the route table you created, complete steps 2 and 3 again to create the **DataRT** route table:
 - a. Name: **DataRT**
 - b. Subscription: **Choose your subscription**
 - c. Resource group: Select **Use existing**, click the drop-down menu and select **WGVNetRG**
 - d. Location: **West US**
6. After you see the **DataRT** route table created (you may need to click **Refresh** again), complete steps 2 and 3 again to create the **WebRT** route table:
 - a. Name: **WebRT**
 - b. Subscription: **Choose your subscription**
 - c. Resource group: Select **Use existing**, click the drop-down menu and select **WGVNetRG**
 - d. Location: **West US**
7. Once route tables are created, your **Route tables** blade should look like the following screenshot:

Route tables
ExamRef

+ Add Assign Tags Columns Refresh

Subscriptions:

3 items

<input type="checkbox"/>	NAME ↑↓	RESOURCE GROUP ↑↓	LOCATION ↑↓
<input type="checkbox"/>	DataRT	WGVNetRG	West US
<input type="checkbox"/>	MgmtRT	WGVNetRG	West US
<input type="checkbox"/>	WebRT	WGVNetRG	West US

Task 2: Add routes to each route table

1. Click on the **DataRT** route table, and click **Routes**.

DataRT - Routes
Route table

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

SETTINGS

- Routes**
- Subnets

2. On the **Routes** blade, click the **+Add** button. Enter the following information, and click **OK**:
 - a. Route name: **DataToInet**
 - b. Address prefix: **0.0.0.0/0**
 - c. Next hop type: **Virtual appliance**
 - d. Next hop address: **10.7.0.4**

Add route
DataRT

* Route name
DataToInet ✓

* Address prefix ⓘ
0.0.0.0/0 ✓

Next hop type ⓘ
Virtual appliance ▼

* Next hop address ⓘ
10.7.0.4 ✓

3. Repeat this procedure to add the **DataToMgmt** route using the following information:
- Route name:
 - Address prefix: **10.7.0.8/29**
 - Next hop type: **Virtual appliance**
 - Next hop address: **10.7.0.4**

Add route
DataRT

* Route name
DataToMgmt ✓

* Address prefix ⓘ
10.7.0.8/29 ✓

Next hop type ⓘ
Virtual appliance ▼

* Next hop address ⓘ
10.7.0.4 ✓

4. Repeat this procedure to add the **DataToWeb** route using the following information:
- Route name: **DataToWeb**
 - Address prefix: **10.7.1.0/24**
 - Next hop type: **Virtual appliance**
 - Next hop address: **10.7.0.4**

Add route
DataRT

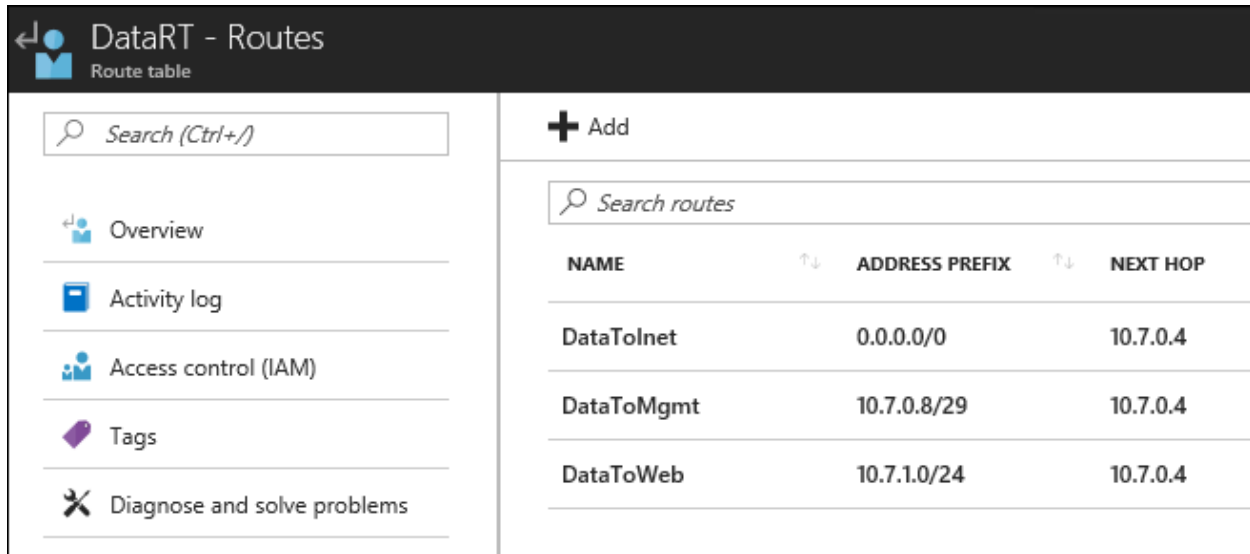
* Route name
DataToWeb ✓

* Address prefix ⓘ
10.7.1.0/24 ✓

Next hop type ⓘ
Virtual appliance ▼

* Next hop address ⓘ
10.7.0.4 ✓

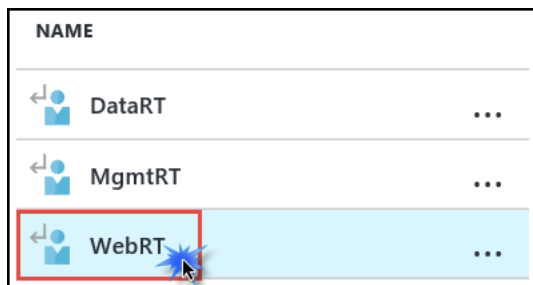
Upon completion, your routes in the **DataRT** route table should look like the following screenshot:



- Using the breadcrumb menu at the top of the portal, click on **Route tables** to go back to that blade.



- Click on **WebRT**, then click **Routes**.



- On the **Routes** blade, click the **+Add** button. Enter the following information, and click **OK**:
 - Route name: **WebToInet**
 - Address prefix: **0.0.0.0/0**
 - Next hop type: **Virtual appliance**
 - Next hop address: **10.7.0.4**



Add route
WebRT


* Route name
WebToInet ✓

* Address prefix ⓘ
0.0.0.0/0 ✓

Next hop type ⓘ
Virtual appliance ▼

* Next hop address ⓘ
10.7.0.4 ✓

8. Repeat this procedure to add the **WebToData** route using the following information:
- Route name: **WebToData**
 - Address prefix: **10.7.2.0/24**
 - Next hop type: **Virtual appliance**
 - Next hop address: **10.7.0.4**



Add route
WebRT

* Route name
WebToData ✓

* Address prefix ⓘ
10.7.2.0/24 ✓

Next hop type ⓘ
Virtual appliance ▼

* Next hop address ⓘ
10.7.0.4 ✓

9. Repeat this procedure add the **WebToMgmt** route using the following information:
- Route name: **WebToMgmt**
 - Address prefix: **10.7.0.8/29**
 - Next hop type: **Virtual appliance**
 - Next hop address: **10.7.0.4**

Upon completion, your routes in the **WebRT** route table should look like the following screenshot:

NAME	ADDRESS PREFIX	NEXT HOP
WebToData	10.7.2.0/24	10.7.0.4
WebToInet	0.0.0.0/0	10.7.0.4
WebToMgmt	10.7.0.8/29	10.7.0.4

10. Using the breadcrumb menu at the top of the portal, click on **Route tables** to go back to that blade.



11. Click on **MgmtRT**, and click **Routes**.

NAME
DataRT
MgmtRT
WebRT

12. On the **Routes** blade, click the **+Add** button. Enter the following information, and click **OK**:

- a. Route name: **MgmtToInet**
- b. Address prefix: **0.0.0.0/0**
- c. Next hop type: **Virtual appliance**
- d. Next hop address: **10.7.0.4**



Add route
MgmtRT

* Route name
MgmtToInet ✓

* Address prefix ⓘ
0.0.0.0/0 ✓

Next hop type ⓘ
Virtual appliance ▼

* Next hop address ⓘ
10.7.0.4 ✓

13. Complete step 12 to add the **MgmtToData** route using the following information:

- a. Route name: **MgmtToData**
- b. Address prefix: **10.7.2.0/24**
- c. Next hop type: **Virtual appliance**
- d. Next hop address: **10.7.0.4**



Add route
MgmtRT

* Route name
MgmtToData ✓

* Address prefix ⓘ
10.7.2.0/24 ✓

Next hop type ⓘ
Virtual appliance ▼

* Next hop address ⓘ
10.7.0.4 ✓

14. Complete step 12 to add the **MgmtToWeb** route using the following information:

- a. Route name: **MgmtToWeb**
- b. Address prefix: **10.7.1.0/24**
- c. Next hop type: **Virtual appliance**
- d. Next hop address: **10.7.0.4**

Upon completion, your routes in the **MgmtRT** route table should look like the following screenshot:

NAME	ADDRESS PREFIX	NEXT HOP
MgmtToData	10.7.2.0/24	10.7.0.4
MgmtToInet	0.0.0.0/0	10.7.0.4
MgmtToWeb	10.7.1.0/24	10.7.0.4

Note: The route tables and routes you have just created are not associated with any subnets yet, so they are not impacting any traffic flow yet. This will be accomplished later in the lab.

Exercise 3: Deploy n-tier application and validate functionality

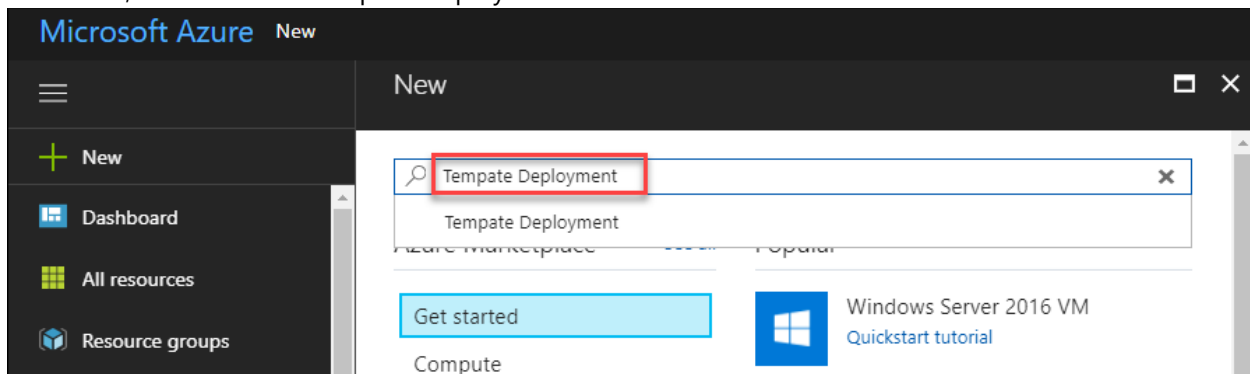
Duration: 60 minutes

In this task, you will provision the CloudShop application using an ARM template deployment. This application has a web tier and a data tier.

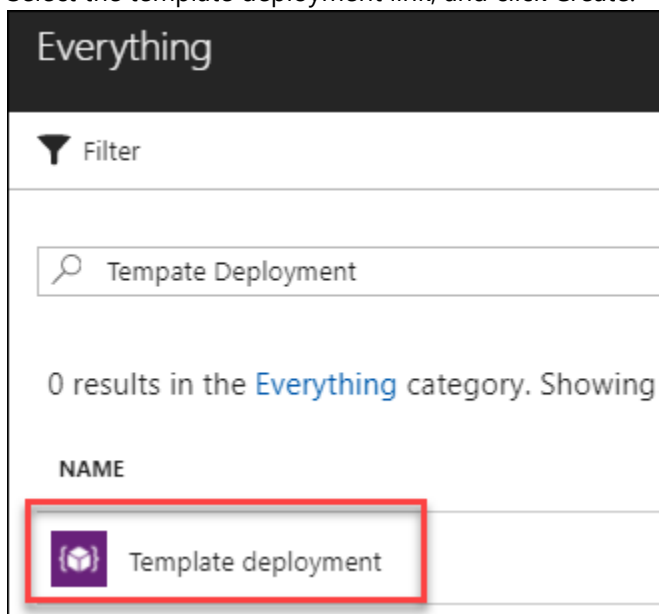
Task 1: Use the Azure portal for a template deployment

NOTE: If you have not downloaded the student files see this section in the before getting started section of this hands-on lab.

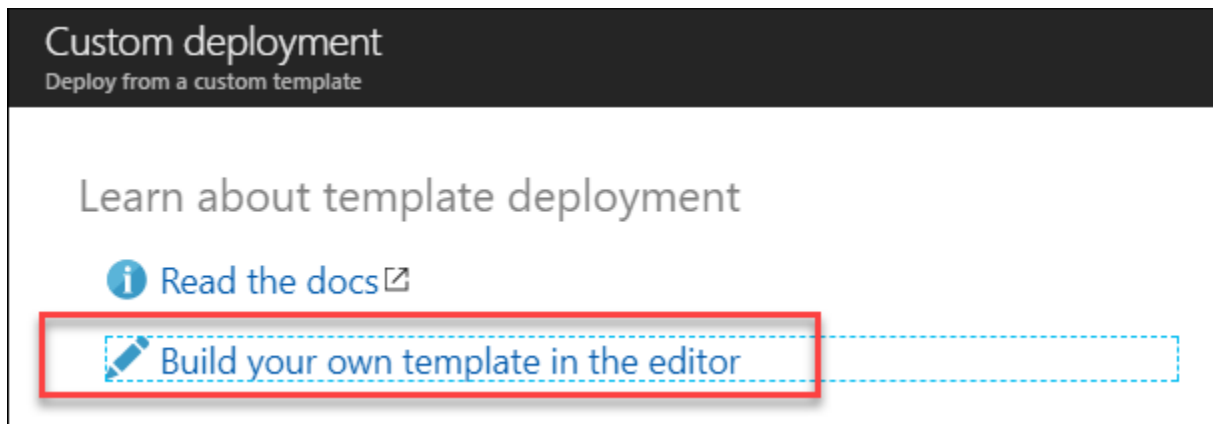
1. On your LABVM, open the **C:\ECN-Hackathon** which contains the student files for this lab.
2. Sign into the Azure portal at <http://portal.azure.com>.
3. Click **New**, and search for template deployment.



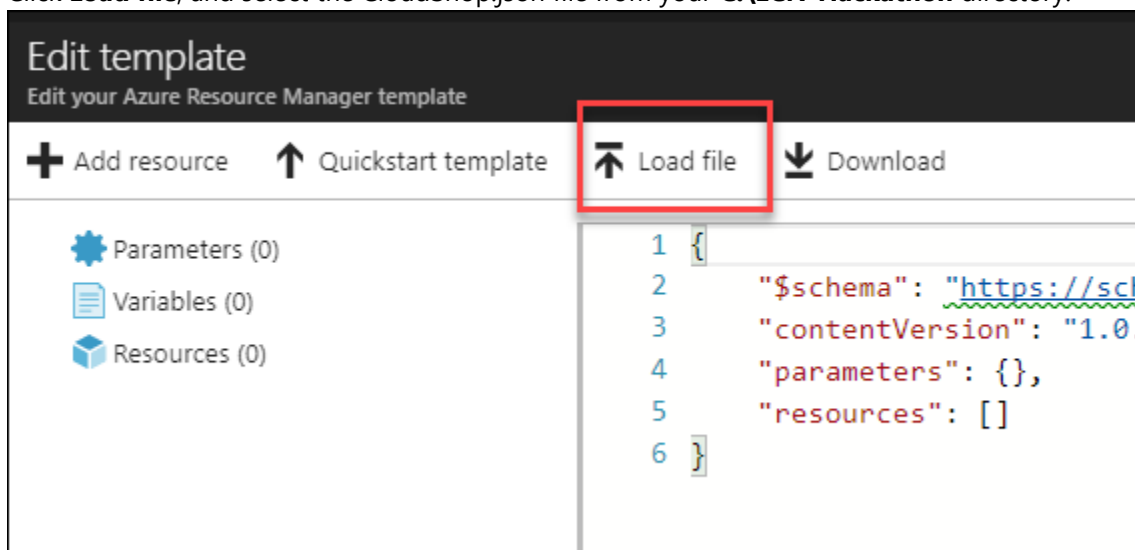
4. Select the template deployment link, and click Create.



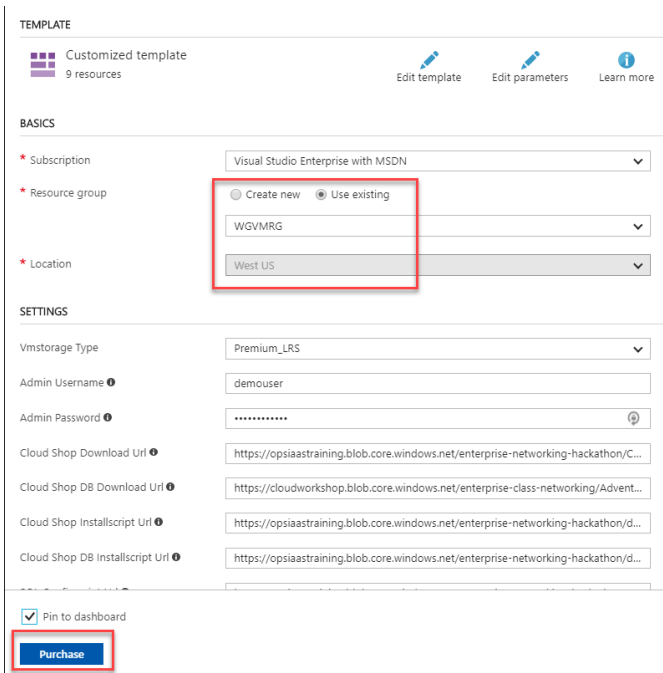
5. On the Custom deployment blade, click **Build your own template in the editor**



6. Click **Load file**, and select the CloudShop.json file from your **C:\ECN-Hackathon** directory.

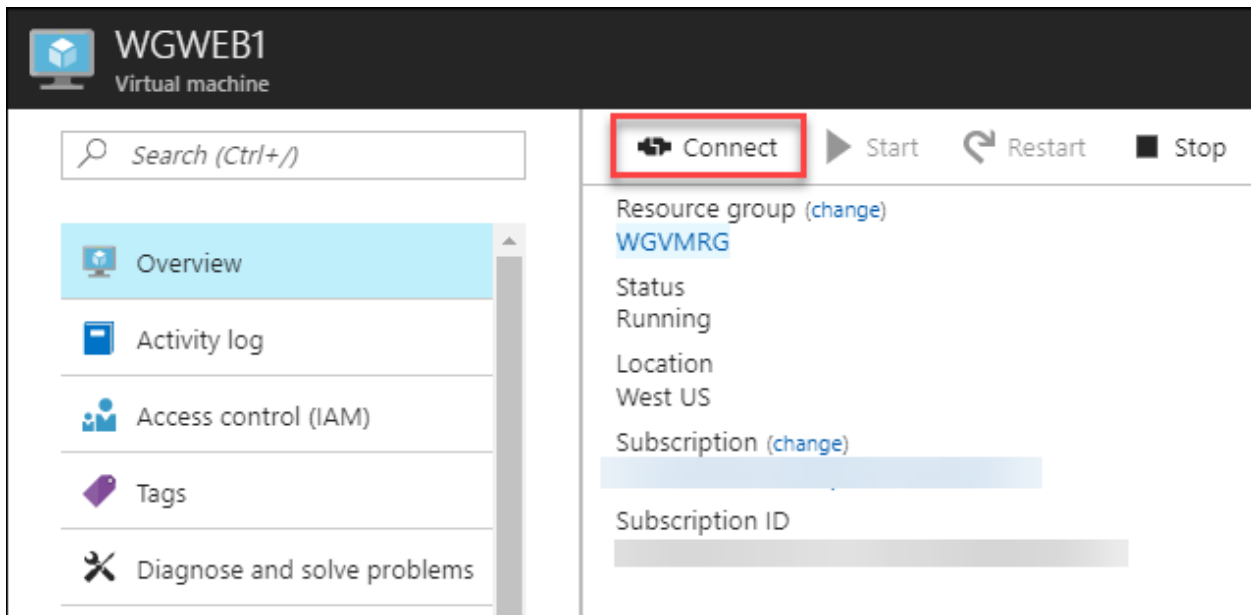


7. Click **Save**.
8. Update the **Custom deployment** blade using the following inputs, agree to the terms, and click **Purchase**. This deployment will take approximately 30-40 minutes.
 - a. Resource Group: Create New / WGVMRG
 - b. Location: West US



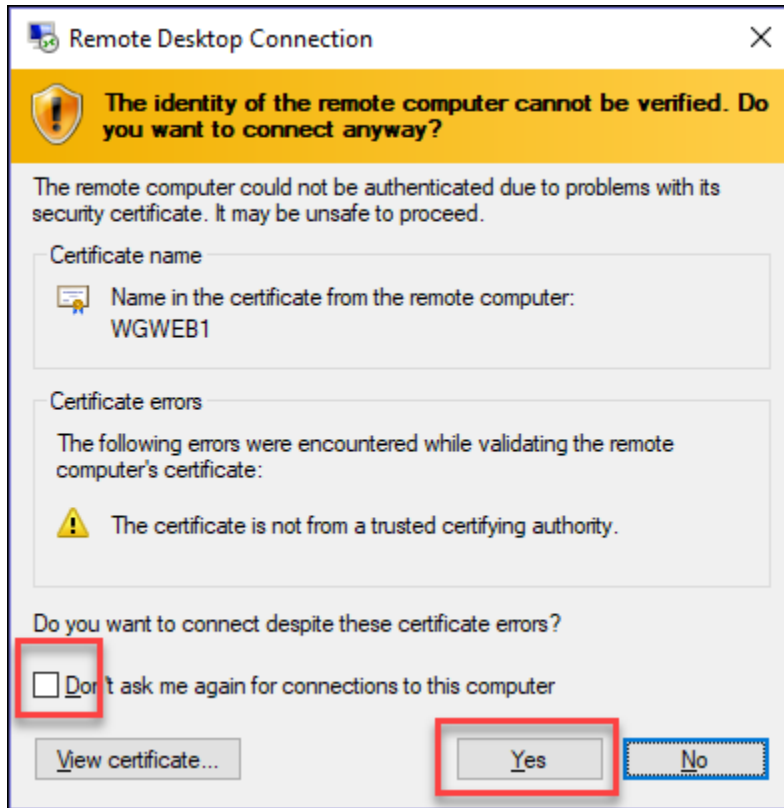
Task 3: Validate the CloudShop application is up after the deployment

1. Using the Azure portal, open the **WGVMRG** Resource group and review the deployment.
2. Open the **WGWEB1** blade in the Azure portal, and click **Connect**.

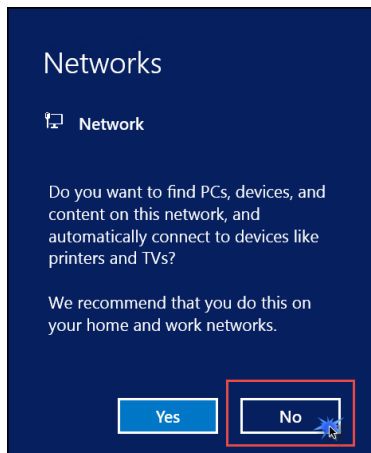


3. Depending on your Remote Desktop protocol client and browser configuration, you will either be prompted to open an RDP file, or you will need to download it and then open it separately to connect.
4. Log in with the credentials specified during creation:
 - c. User: **demouser**
 - d. Password: **demo@pass123**

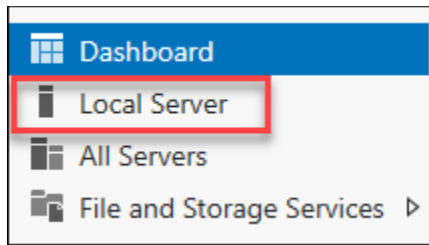
- You will be presented with a Remote Desktop Connection warning because of a certificate trust issue. Click **Yes** to continue with the connection.



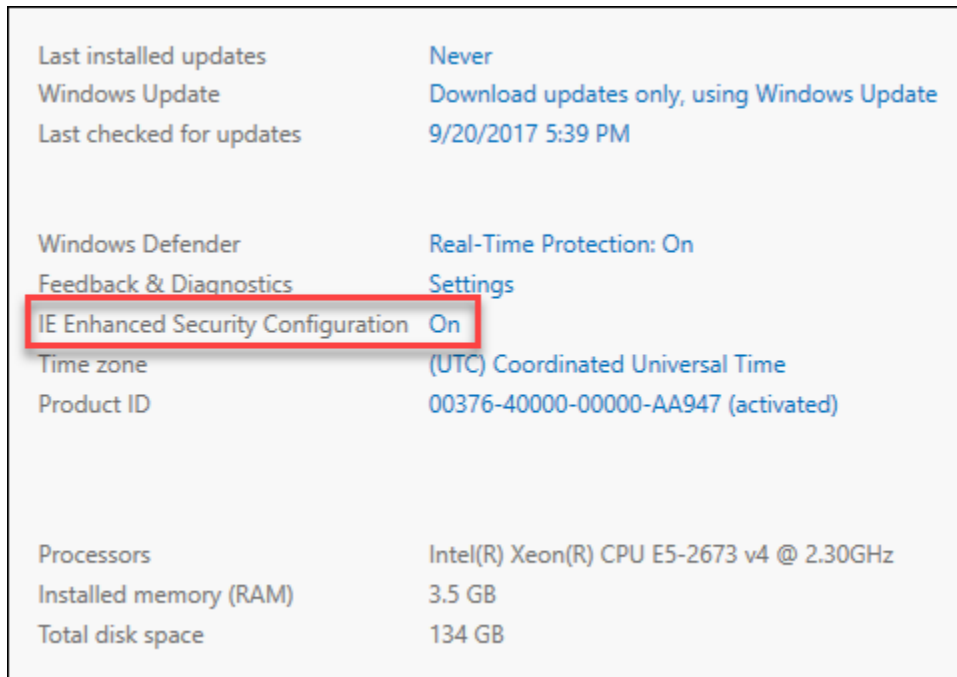
- When logging on for the first time, you will see a prompt on the right asking about network discovery. Click **No**.



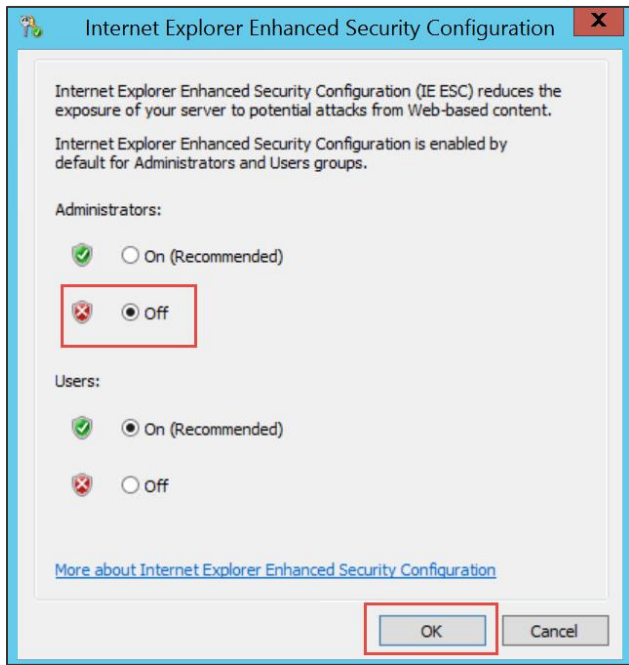
- Notice that Server Manager opens by default. On the left, click **Local Server**.



8. On the right side of the pane, click **On** by **IE Enhanced Security Configuration**.



9. Change to **Off** for Administrators, and click **OK**.

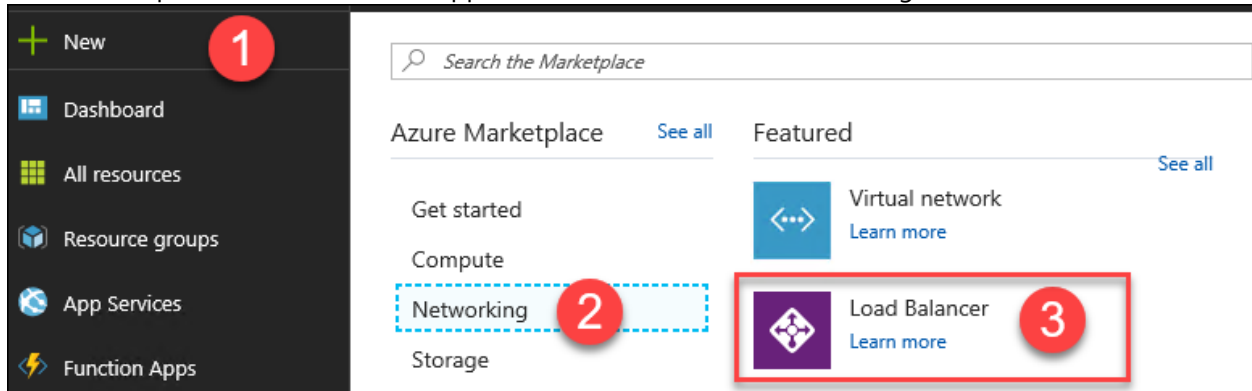


10. You will now ensure the CloudShop application is up and running. Open Internet explorer, and browse to both the WGWEB1 and WGWEB2 servers.

```
http://wgweb1
http://wgweb2
```

Task 4: Create a load balancer to distribute load between the web servers

1. In the Azure portal, click **New** in the upper left-hand corner, then Networking, Load Balancer.



2. In the **Create load balancer** blade, enter the following values:
 - a. Name: **WGWEBLB**
 - b. Type: **Internal**
 - c. **Virtual network: WGVNet**
 - d. **Subnet: WebTier**

- e. **IP address assignment:** click **Static** and enter the IP address **10.7.1.10**
- f. **Subscription:** choose your subscription
- g. **Resource group:** click **Use existing** and select **WGVMRG**
- h. **Location:** **West US**.

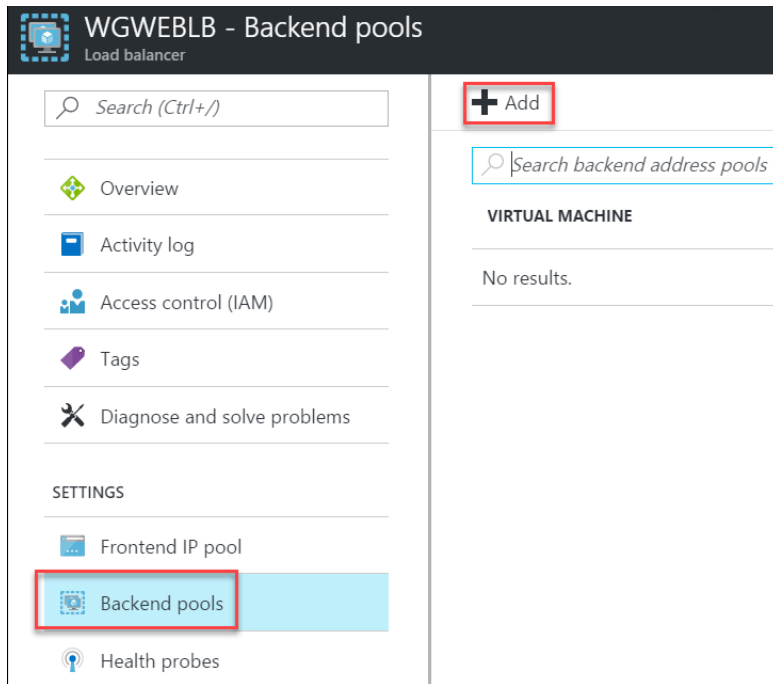
Ensure your **Create load balancer** dialog looks like the following, and click **Create**.

The screenshot shows the 'Create load balancer' dialog box with the following configuration:

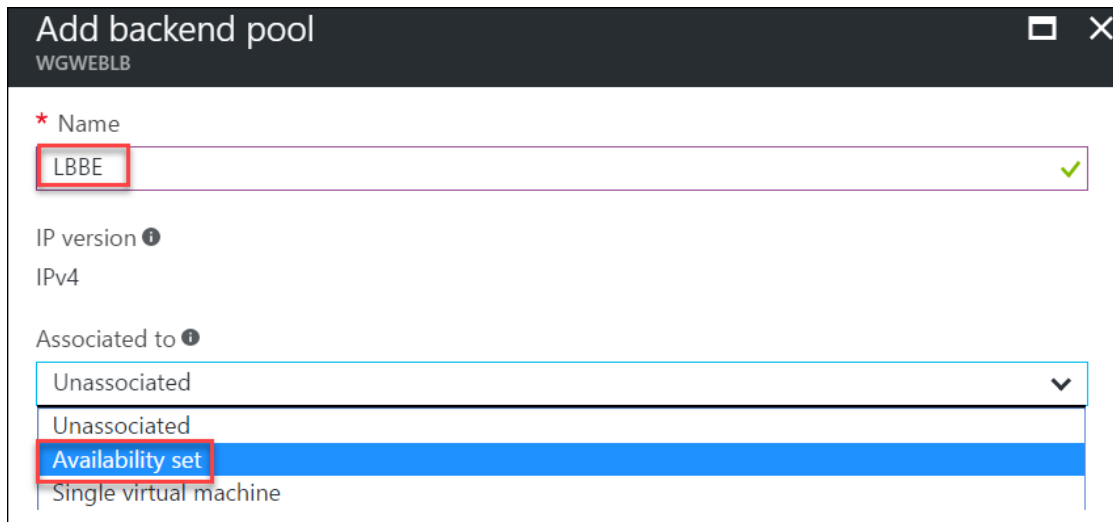
- Name:** WGWEBLB (checked)
- Type:** Internal (selected)
- Virtual network:** WGVNet
- Subnet:** WebTier (10.7.1.0/24)
- IP address assignment:** Static (selected)
- Private IP address:** 10.7.1.10 (checked)
- Subscription:** (empty)
- Resource group:** Use existing (selected), WGVMRG
- Location:** West US

Task 5: Configure the load balancer

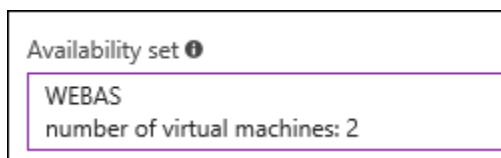
1. Open the WGWEBLB load balancer in the Azure portal.
2. Click **Backend pools**, and click **+Add** at the top.



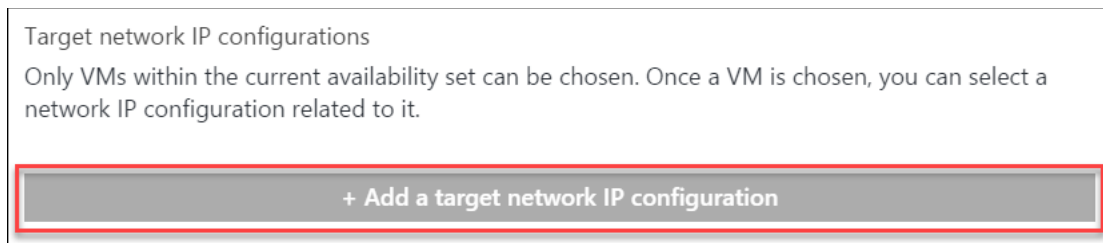
3. Enter **LBBE** for the pool name. Under **Associated to**, choose **Availability set**.



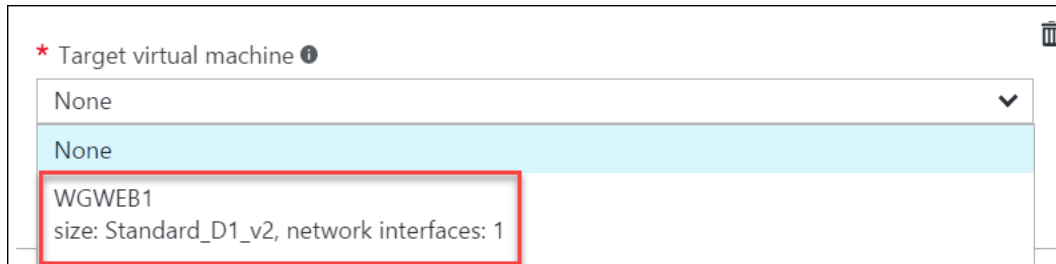
4. Next, select the **WEBAS** Availability Set.



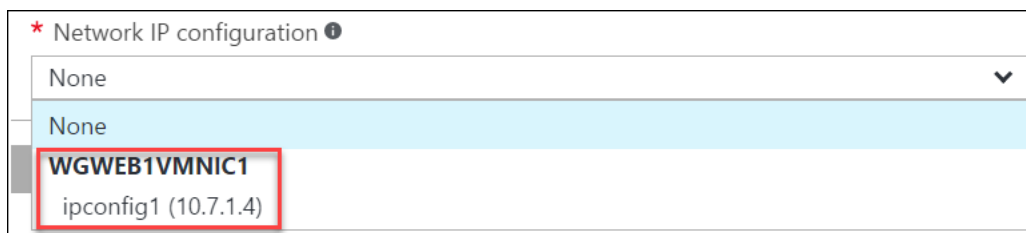
5. Under **Target network IP configurations**, click + **Add a target network IP configuration**.



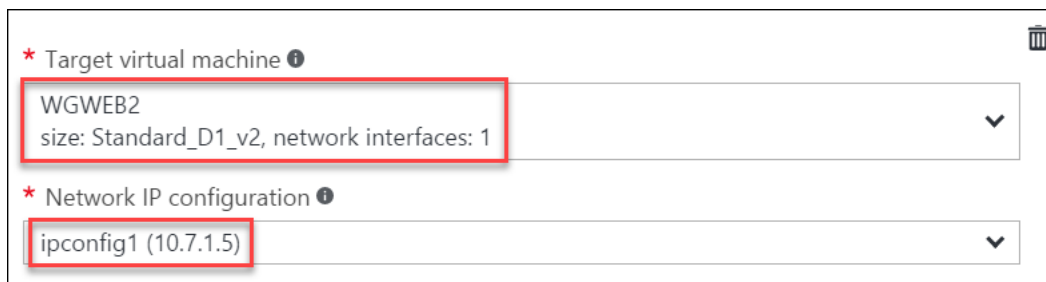
- Under **Target virtual machine**, choose **WGWEB1**.



- Under **Network IP configuration**, choose **WGWEB1VMNIC1**.



- Click + **Add a target network IP configuration** repeating these steps, but this time, adding **WGWEB2** along with its IP configuration.



- Then, click **OK**.

- Wait to proceed until the Backend pool configuration is finished updating.

+ Add			
🔍 Search backend address pools			
VIRTUAL MACHINE	STATUS	NETWORK INTERFACE	PRIVATE IP ADDRESS
▼ LBBE (2 virtual machines)			
WGWEB1	-	WGWEB1VMNIC1	10.7.1.4
WGWEB2	-	WGWEB2VMNIC1	10.7.1.5

11. Next, under **Settings** click on **Health Probes**. Click **+Add**, and use the following information to create a health probe.

- a. Name: **HTTP**
- b. Protocol: **HTTP**

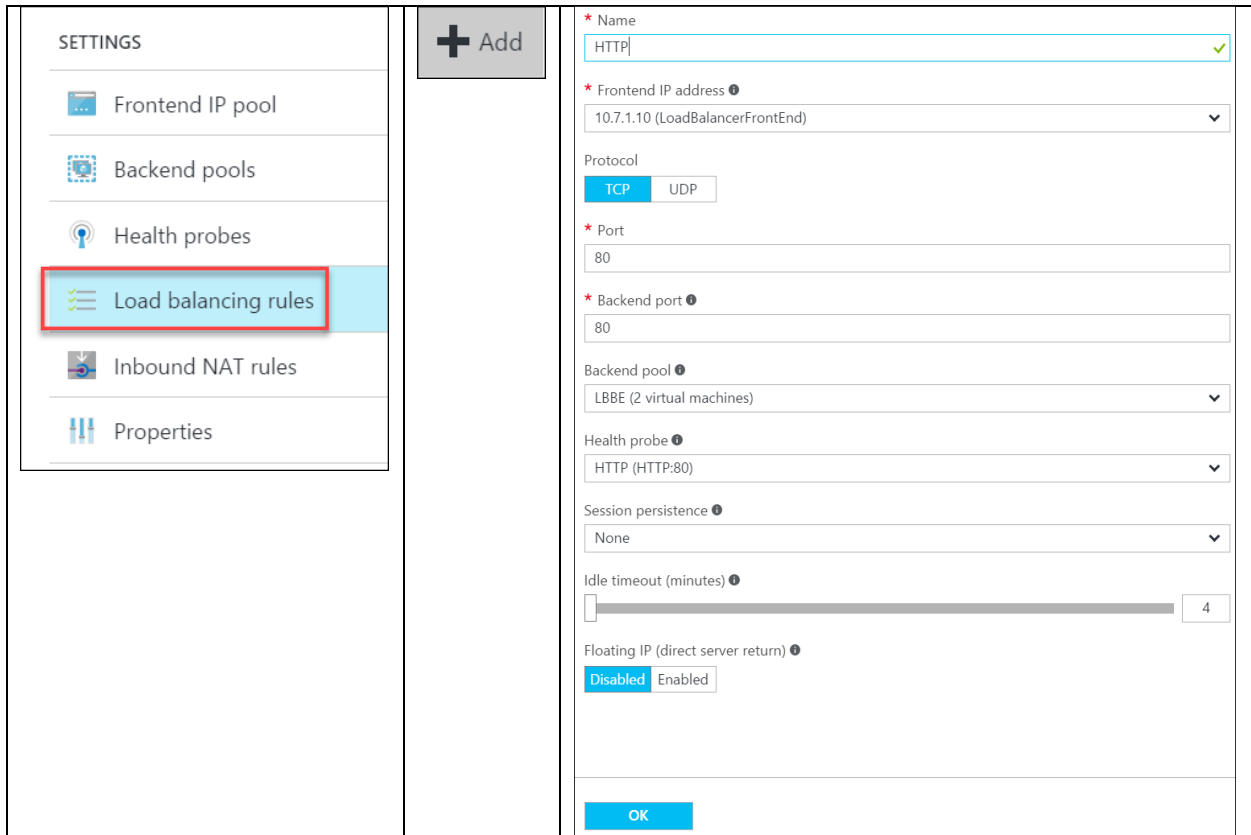
The screenshot shows the 'Add health probe' configuration window in the Azure portal. On the left, the 'SETTINGS' menu has 'Health probes' selected. The main window contains the following fields:

- Name:** HTTP
- Protocol:** HTTP (selected from a dropdown menu)
- Port:** 80
- Path:** /
- Interval:** 5 seconds
- Unhealthy threshold:** 2 consecutive failures

The 'OK' button at the bottom is highlighted with a red box.

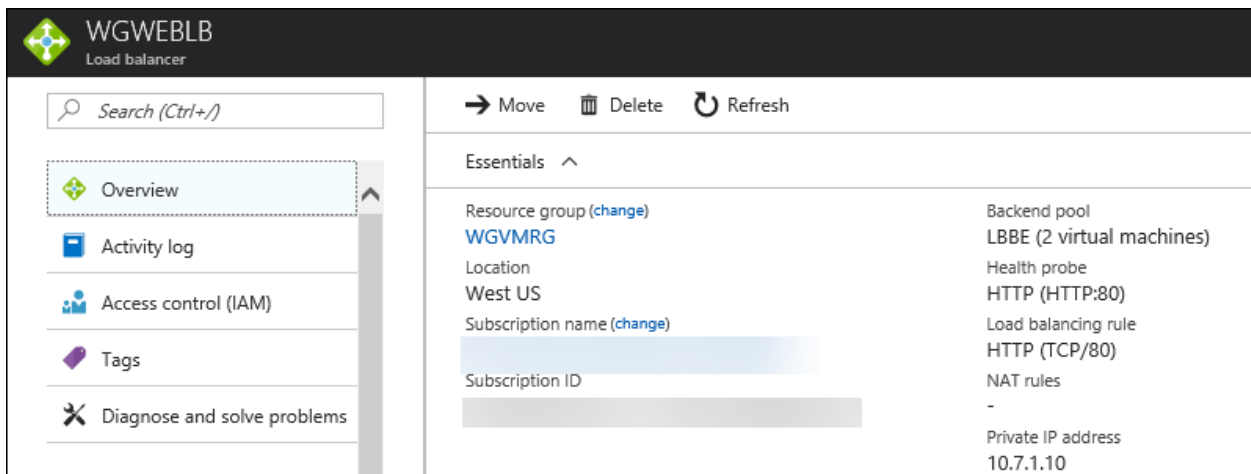
12. Click **OK**.

13. After the Health probe has updated. Click **Load balancing rules**. Click **+Add** and complete the configuration as shown below followed by clicking **OK**.



It will take 2-3 minutes for the changes to save.

14. The **Essentials** panel shows you a high-level view of how many virtual machines are in the backend pool and other information.

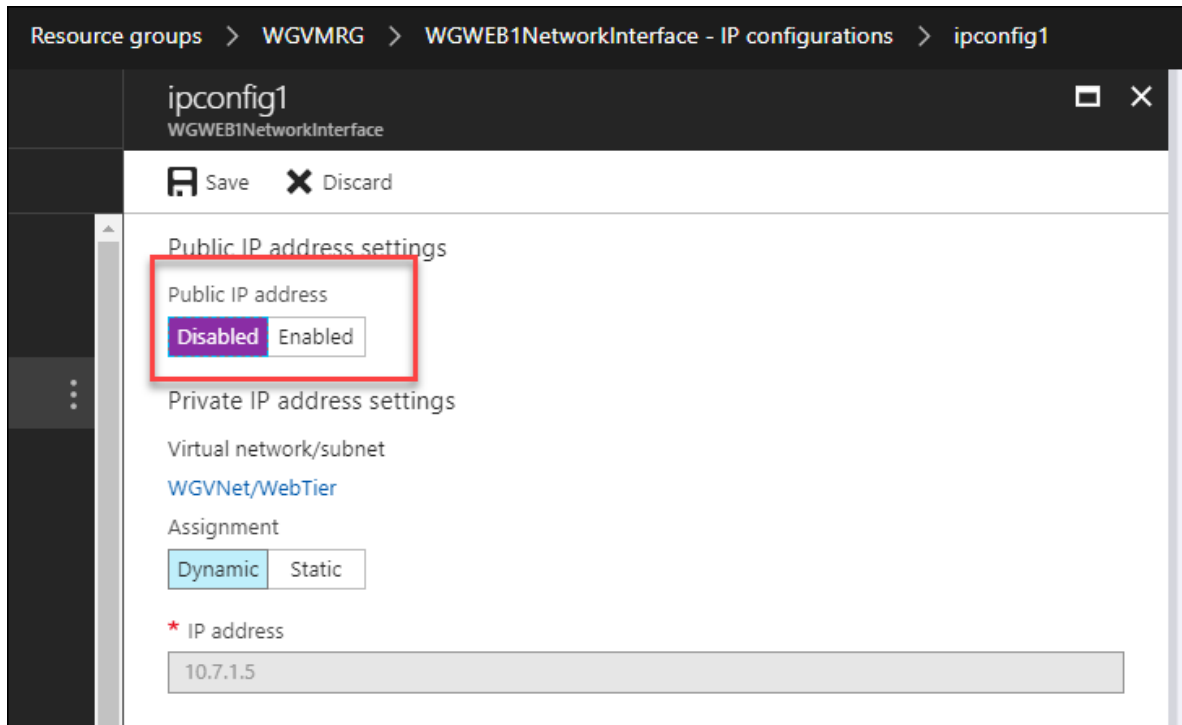


15. From an RDP session to WGWEB1, open your browser and point it at <http://10.7.1.10>. Press F5 until you see both servers responding.

CloudShop Demo - Products - running on WEB1

CloudShop Demo - Products - running on WEB2

16. Using the portal, disassociate the Public IP from the NIC of WGWEB1.



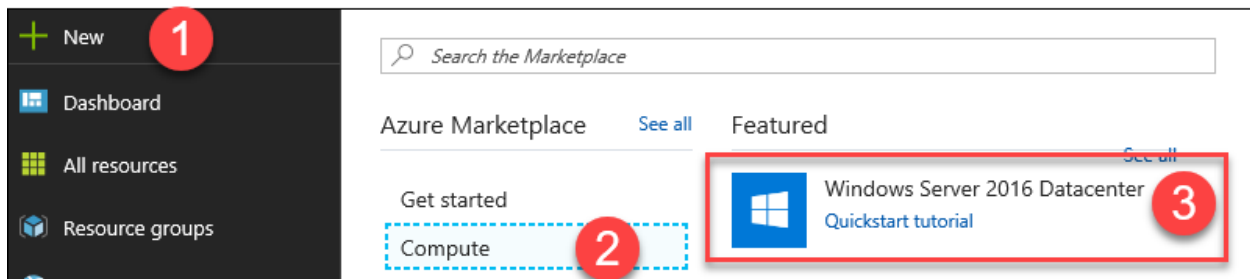
Exercise 4: Build the management station

Duration: 15 minutes

In this exercise, management of the Azure-based systems will only be available from a management 'jump box.' In this section, you will provision this server.

Task 1: Build the management VM

1. In the Azure portal, click on the **New** button in the upper left of the portal. In the Marketplace category list, choose **Compute**. In the Featured Apps list, click **Windows Server 2016 Datacenter**.



2. On the **Basics** blade, shown in the following screenshot, enter the following information, and click **OK**.
 - a. Name: **WGMGMT1**
 - b. VM disk type: **SSD**
 - c. User name: **demouser**
 - d. Password: **demo@pass123**
 - e. Subscription: **Choose your subscription**
 - f. Resource group: Choose **Create new** and enter **WGMGMTRG**
 - g. Location: **West US**

The image shows a 'Basics' configuration window with the following fields and values:

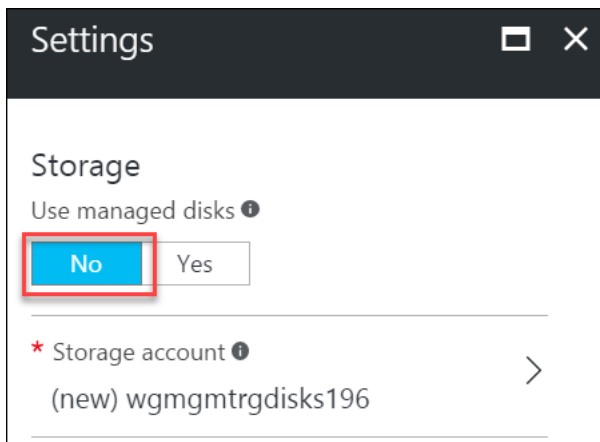
- Name:** WGMGMT1 (with a green checkmark)
- VM disk type:** SSD (dropdown menu)
- User name:** demouser
- Password:** (masked with dots)
- Confirm password:** (masked with dots)
- Subscription:** (dropdown menu)
- Resource group:** Create new Use existing. Dropdown menu shows WEGMGMTRG (with a green checkmark).
- Location:** West US (dropdown menu)

3. On the **Choose a size** blade, click **F1S** (you will need to click **View all** and scroll down to find the F1S size). then Click **Select**.

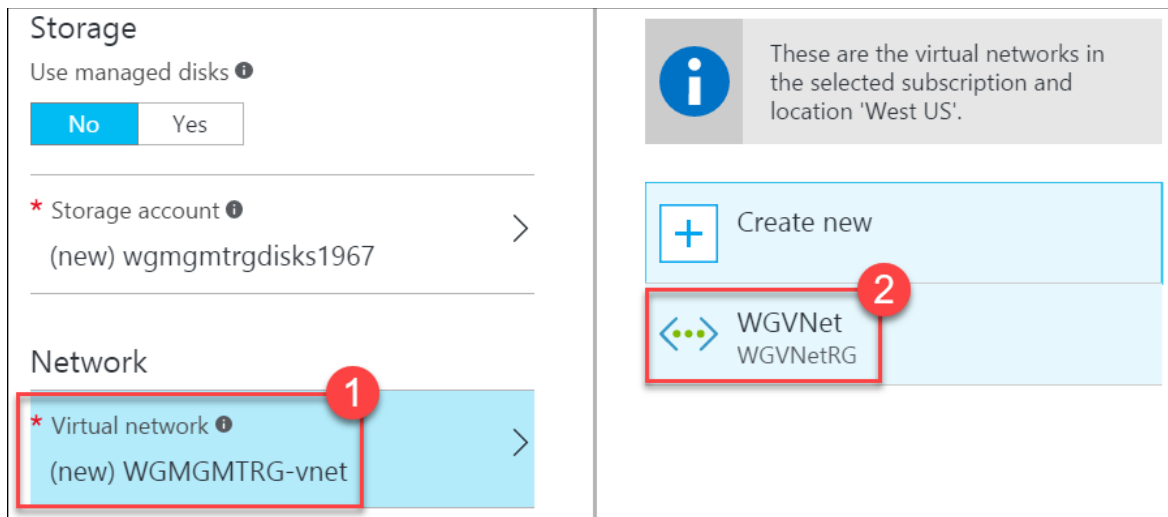
F1S Standard		F2S Standard		F4S Standard	
1	Core	2	Cores	4	Cores
2	GB	4	GB	8	GB
	2 Data disks		4 Data disks		8 Data disks
	3200 Max IOPS		6400 Max IOPS		12800 Max IOPS
	Load balancing		Load balancing		Load balancing
	Premium disk support		Premium disk support		Premium disk support
46.13 USD/MONTH (ESTIMATED)		92.26 USD/MONTH (ESTIMATED)		185.26 USD/MONTH (ESTIMATED)	

Select

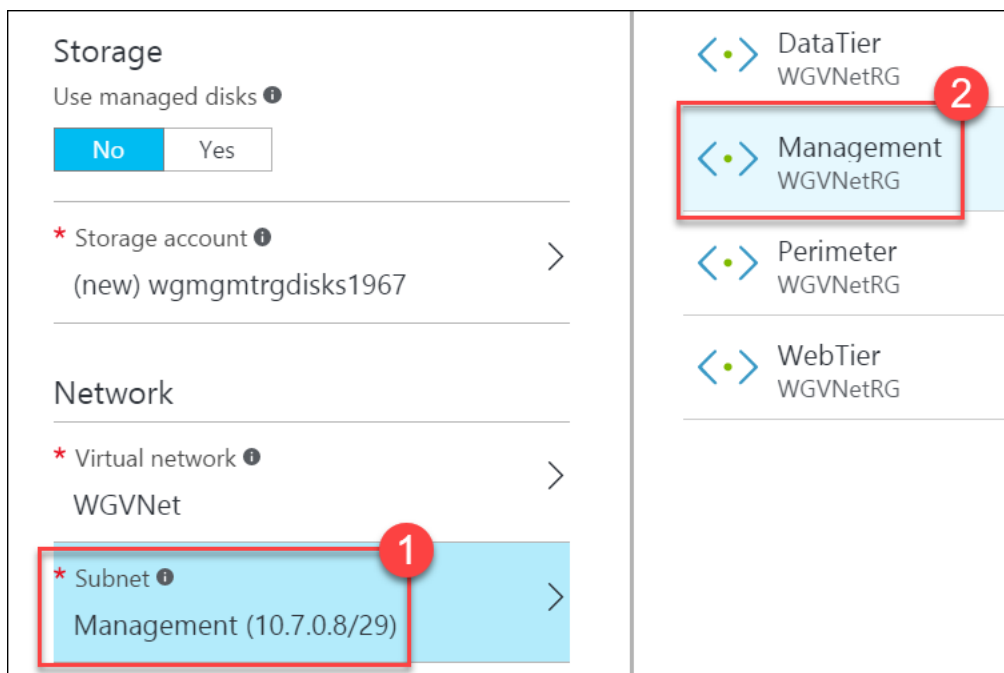
- On the **Settings** blade, under **Storage**, select **No** for **Use managed disks**.



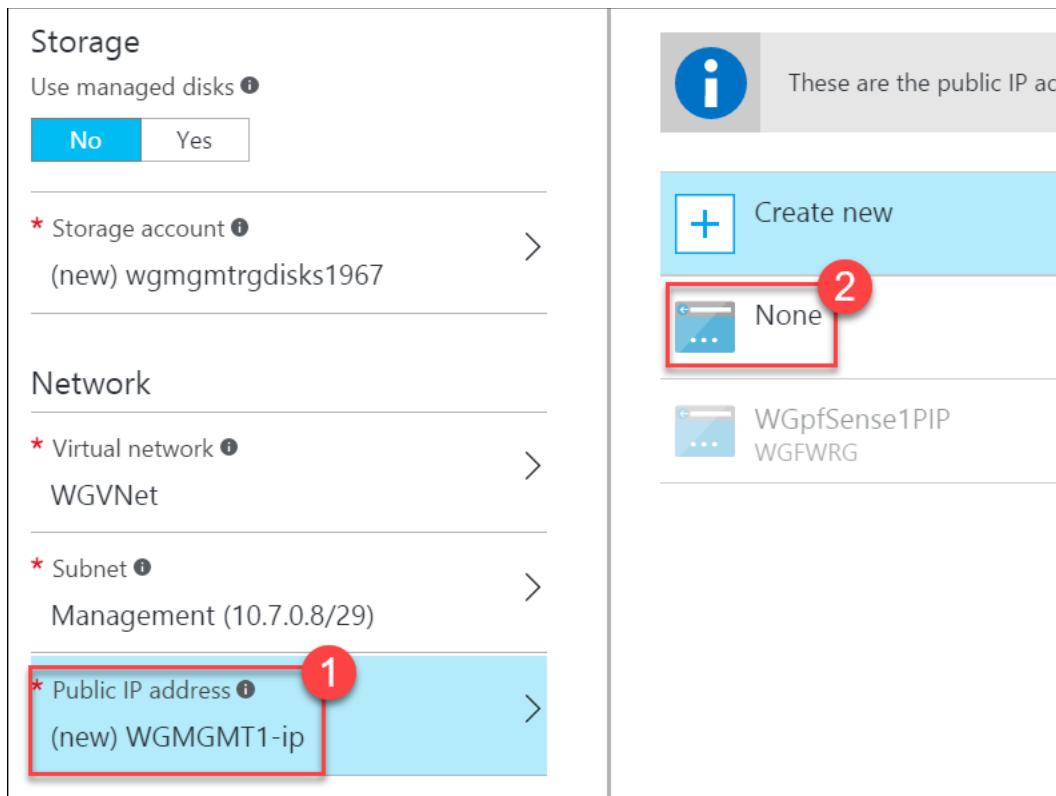
- Under **Network**, click on the **Virtual network** section. On the **Choose virtual network** blade, click on **WGVNet**.



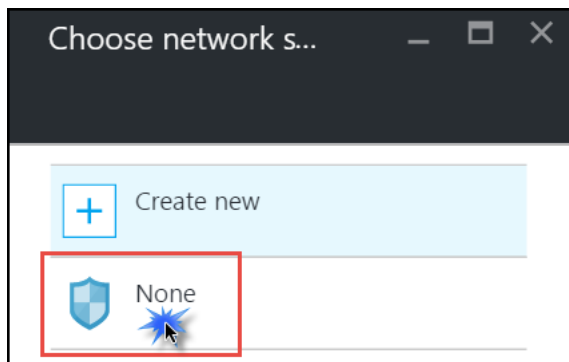
6. In the **Subnet** section, click the subnet that was chosen, and choose **Management**.



7. In the **Public IP address** section, click the name that was pre-populated. Then, click the **Choose Public IP address** blade, and click **None**.

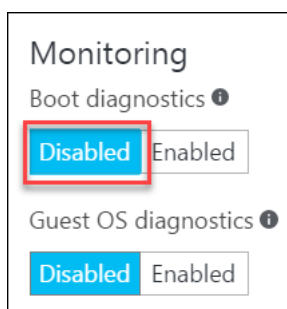


- Click on the **Network security group (firewall)** section, and in the **Choose network security group** blade, click **None**.

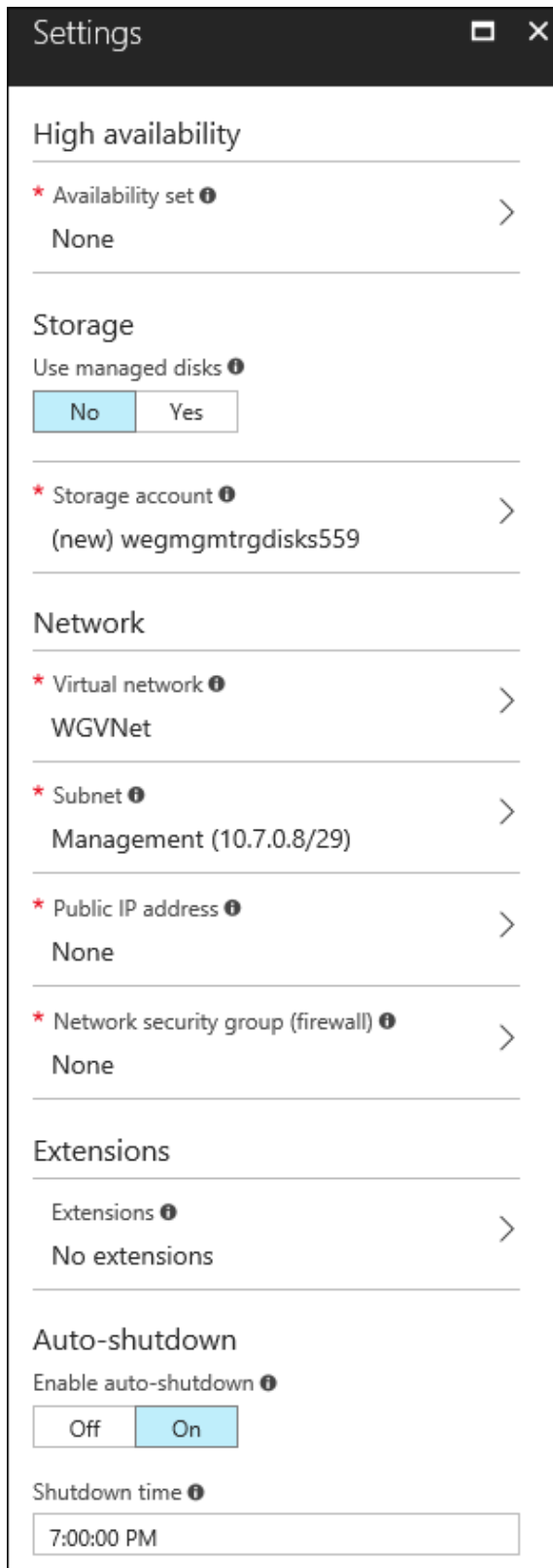


Note: Because this server has no Public IP address and is only accessible through a firewall, an NSG is not required.

- Under **Monitoring**, for **Boot diagnostics**, choose **Disabled**.



10. The remaining sections of the **Settings** blade are correct. Click **OK**. See the following screenshot for details.



11. On the **Summary** blade, ensure the validation passes, and click **Create**. The virtual machine will take 5-10 minutes to provision.

Exercise 5: Provision and configure partner firewall solution

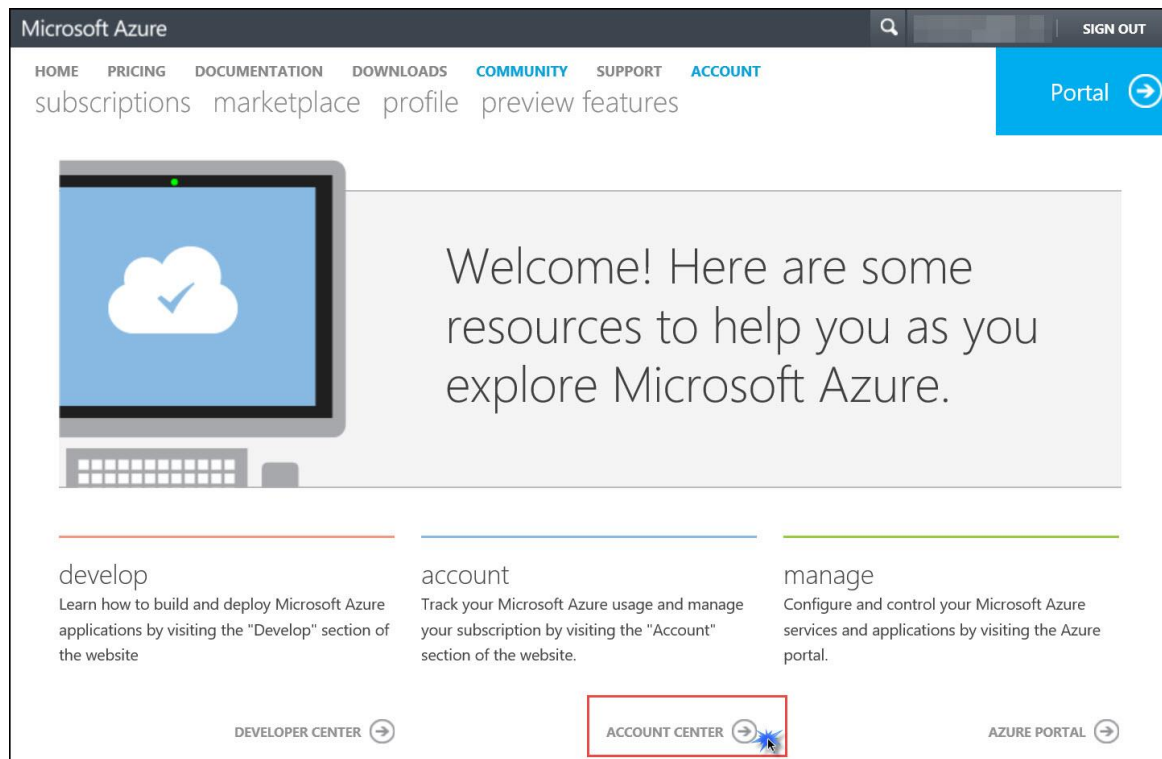
Duration: 15 minutes

In this exercise, you will provision and configure a pfSense firewall appliance in Azure. This appliance is offered as a 'Free Trial' but deployments with only a single CPU core are free. Our deployment will be using a single CPU core. However, 'Free Trials' in Azure require your subscription does not have a spending cap in place and a credit card is associated with your subscription. The first task within this exercise walks through removing a spending cap and associating a credit card with the subscription. If your subscription already has no spending cap and has a credit card associated with it, you can skip the first section.

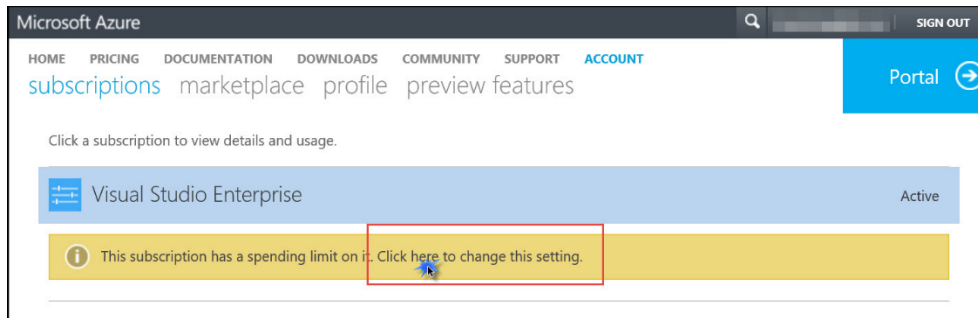
Task 1: Removing a spending cap and associating a credit card with your subscription

1. Navigate to the Azure Account Center using the link below, and click on **Account Center** link. You may need to log on. If so, use the same credentials you are using to log into the Azure portal.

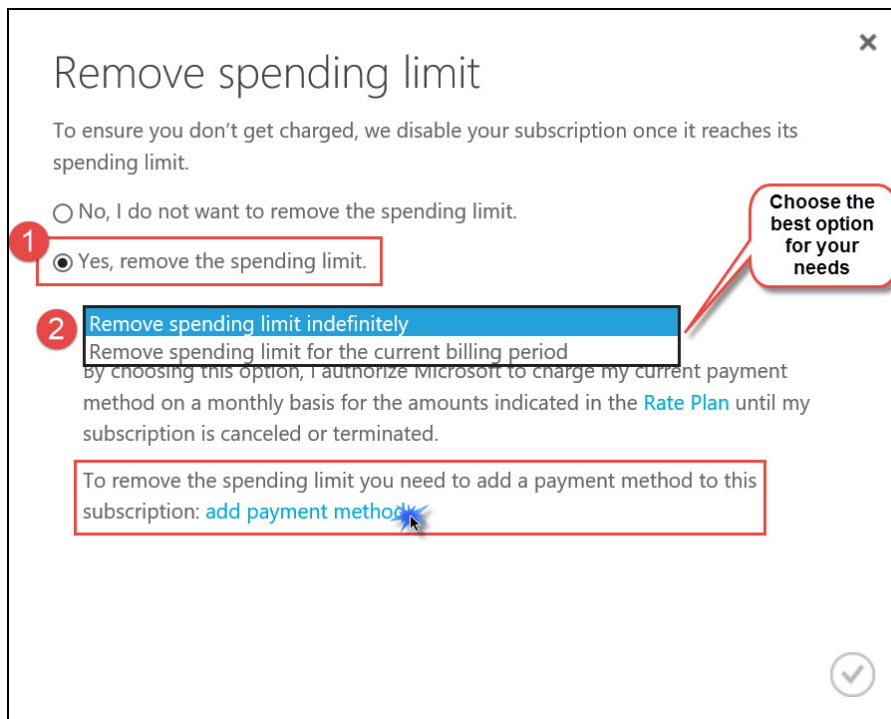
<https://account.windowsazure.com/Home/Index>



2. Here, you will see your subscription and a message indicating it has a spending limit on it. Click to change this limit. See the following screenshot for details.

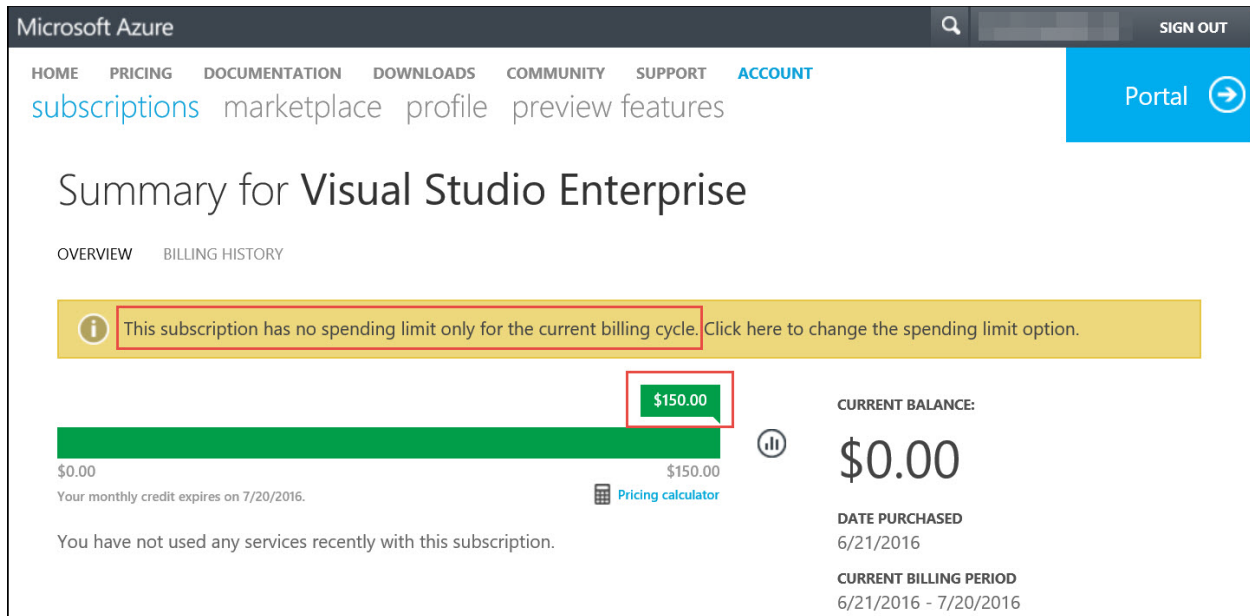


- On the **Remove spending limit** dialog, select **Yes, remove the spending limit**, and choose which option is best for your needs. Then, click **add payment method**.



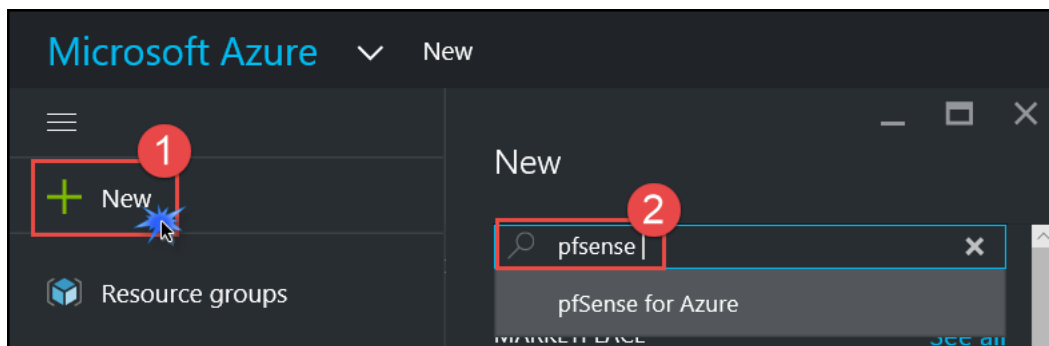
- On the **Choose a payment method** dialog enter your credit card information, and click **Next**.
- Now the **Remove spending limit** dialog should reflect your credit card info. Click the check mark in the lower right.
- After a few minutes, your subscription will reflect the new status.

NOTE: the credit associated with the subscription remains, and this will be consumed first.



Task 2: Provision the firewall appliance

1. Within the Azure portal, click **New** in the upper left corner of the portal. In the search dialog, type **pfSense** and press the **Enter** key on your keyboard.



2. A list of Marketplace offers is returned. Find the one called **pfSense for Azure**, and click that option.



3. The marketplace description of the offer is returned. pfSense is offered as a free trial but deployments with only a single CPU core are free. Click **Create**.
4. On the **Basics** blade, shown in the following screenshot, enter the following information:
 - a. Name: **WGpfSense1**
 - b. VM disk type: **SSD**
 - c. User name: **demouser**
 - d. Authentication type: Select **Password**
 - e. Password: **demo@pass123**
 - f. Subscription: **Select your subscription**
 - g. Resource group: Select **Create New** and enter the name **WGFWRG**
 - h. Location: **West US**

Click **OK**.

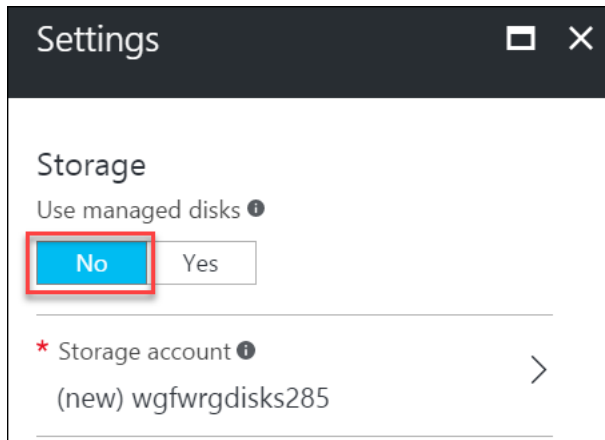
The screenshot shows the 'Basics' configuration window with the following fields and values:

- Name:** WGpfSense1 ✓
- VM disk type:** SSD ✓
- User name:** demouser ✓
- Authentication type:** Password ✓
- Password:** demo@pass123 ✓
- Confirm password:** demo@pass123 ✓
- Subscription:** (dropdown menu)
- Resource group:** Create new (selected), WGFWRG ✓
- Location:** West US ✓

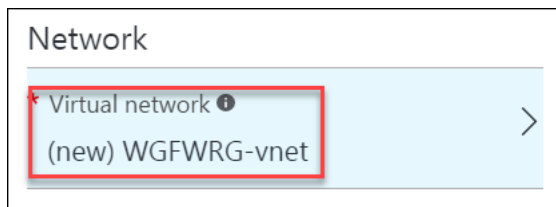
- Choose the **DS1_V2 Standard** instance size on the **Size** blade, and click **Select** at the bottom of the blade.

Note: You may have to click the **View All** link to see the instance sizes.

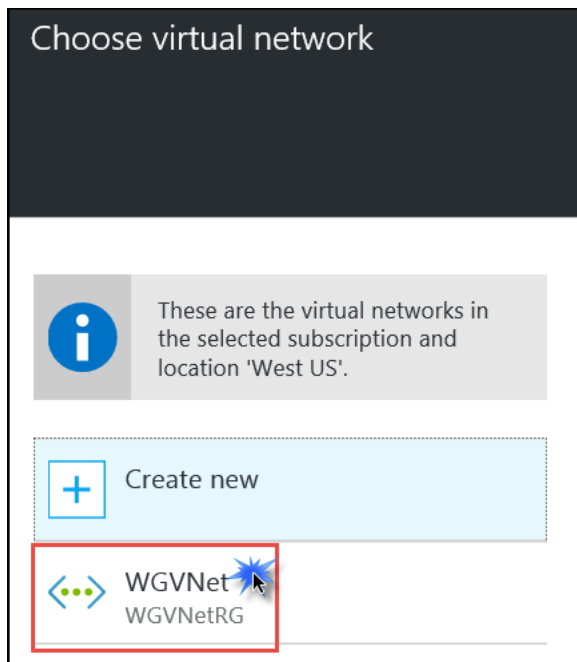
- On the **Settings** blade, choose **No** for **Use managed disks**. If the **Storage account** section shows **Create new**, then click it and walk through the new storage account creation steps. click the virtual network name that was pre-populated.



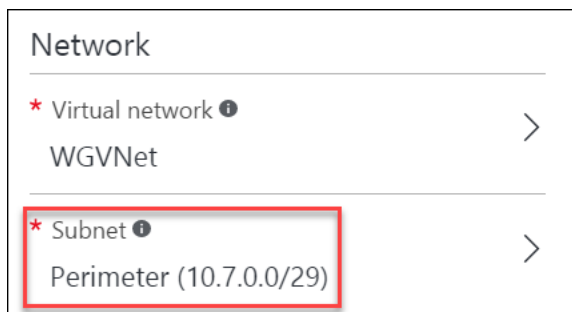
- Under **Network**, click the virtual network name that was pre-populated.



- The **Choose virtual network** blade opens. Click on **WGVNet** to select the virtual network you created earlier in this hands-on lab-step by-step.



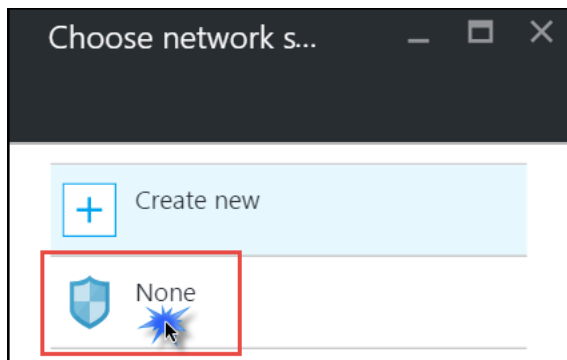
9. Back on the **Settings** blade, take note of the subnet that was selected. If it is not set to **Perimeter** then click on the subnet name and change it **Perimeter**.



10. Back on the **Settings** blade, under **Public IP Address**, click on the name that was pre-assigned. This opens the **Choose Public IP address** and **Create Public IP address** blades. Change the name to **WGpfSense1PIP** and under **Assignment** select **Static**. Click **OK**.

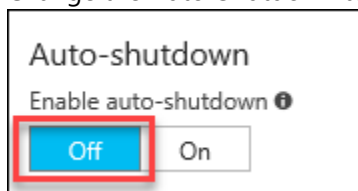


11. Back on the **Settings** blade, click the **Network security group** section, and in the **Choose network security group** blade, click **None**.



Note: This server is a hardened firewall that has built-in security at the network layer. As such, an NSG is not required.

12. Change the Auto-Shutdown to **Off**.

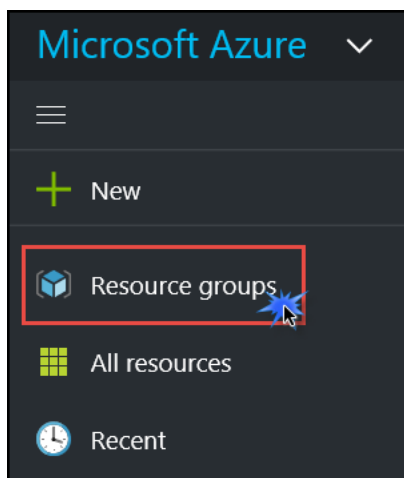


13. All remaining settings on the **Settings** blade are correct. Click **OK** to accept these settings.
14. On the **Summary** blade, ensure the validation passes, and then click **Create**.

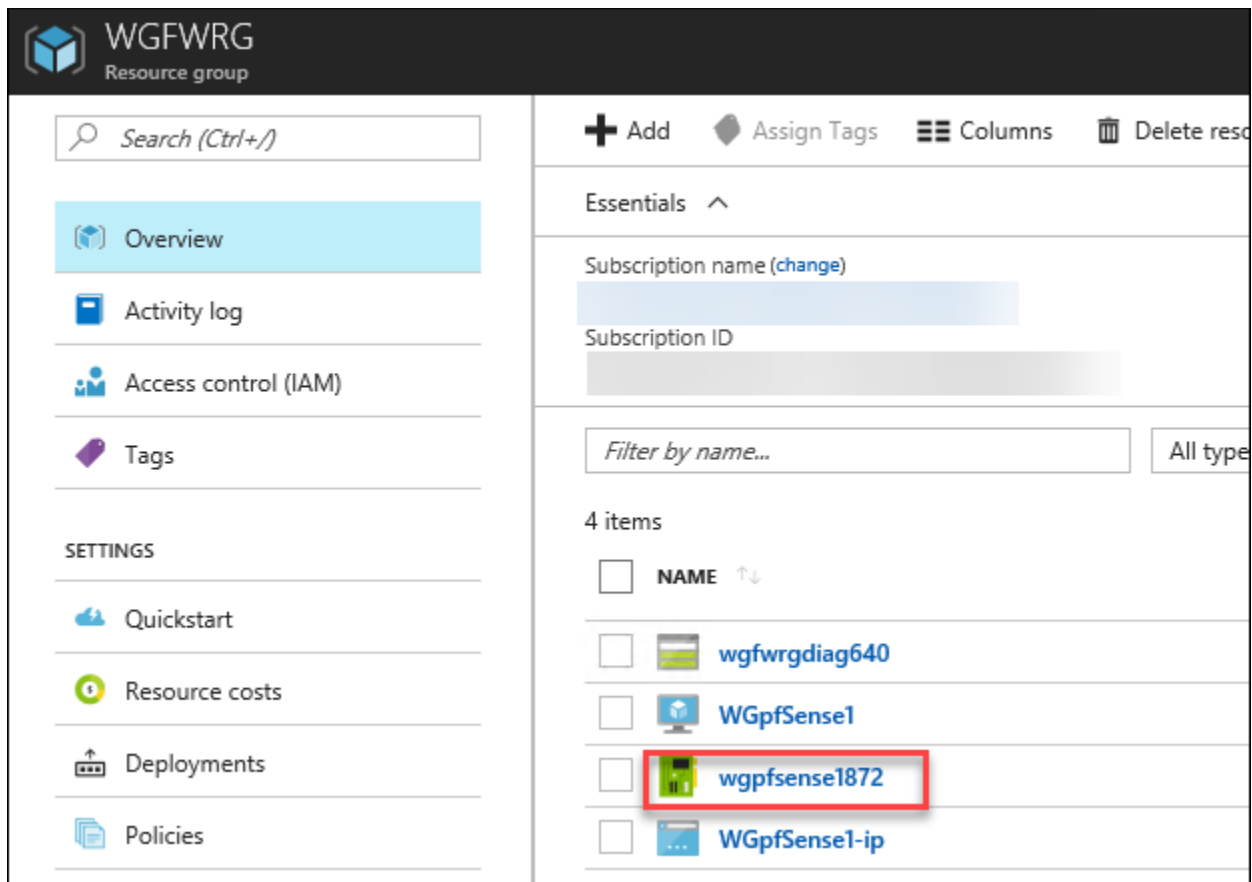
Task 3: Enable IP forwarding on the firewall network interface

Within 1-2 minutes, the resource group **WGFWRG** will be created and the appliance will be in the creation process. Next, we will edit settings on the network interface associated with the firewall.

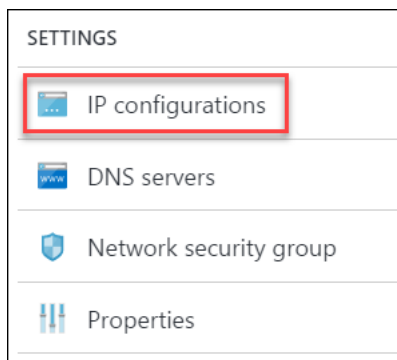
1. On the main Azure menu click on **Resource groups**.



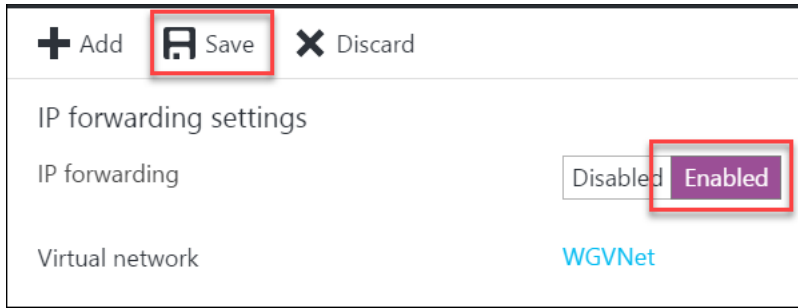
2. Click on the **WGFWRG** resource group. This resource group contains the objects associated with the firewall appliance. Click on the network interface.



- This opens the **Essentials** and **Settings** blade for the network interface. On the **Settings** blade, click **IP configurations**.



- On the **IP configurations** blade, beside **IP forwarding settings**, click **Enabled**. Then, click **Save** at the top of the blade.



Exercise 6: Configure the firewall to control traffic flow

Duration: 30 minutes

In this exercise, you will configure the firewall appliance to allow the necessary traffic to flow so that:

- The web application is accessible from the Internet.
- Application traffic can flow between the tiers.
- An administrator can RDP into the management station, and from there, RDP into other servers for management purposes.

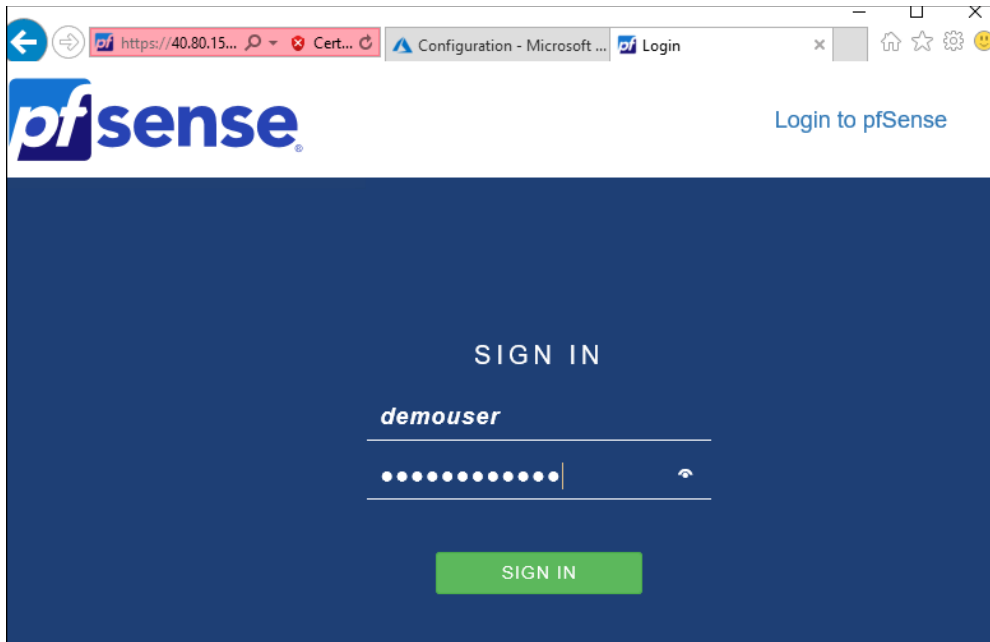
Task 1: Log on to pfSense and add aliases

1. When the provisioning of the pfSense appliance is finished, its **Essentials** blade and **Settings** blade will open in the portal. Take note of the **Public IP address** in the **Essentials** blade.

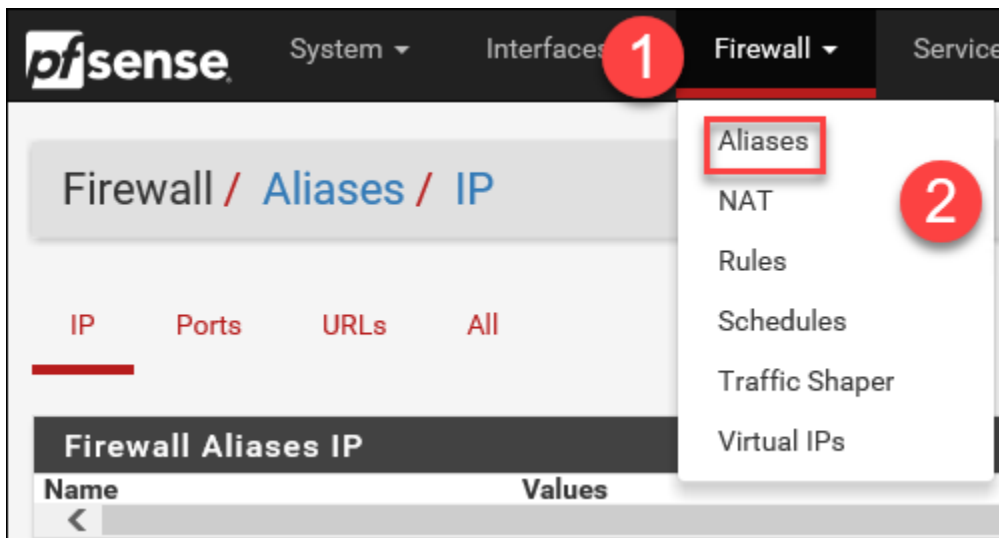
Resource group (change) WGFWRG	Computer name WGpfSense1
Status Running	Operating system Linux
Location West US	Size [REDACTED]
Subscription (change) [REDACTED]	Public IP address 40.80.154.77
Subscription ID [REDACTED]	Virtual network/subnet WGVNet/Perimeter

2. Open a web browser, and navigate to the Public IP address listed on the appliance essentials blade. **You will receive a certificate warning.** Continue to the page. You should now see the pfSense management GUI and the logon screen. Enter the credentials you provided when you provisioned the appliance.
 - a. Username: **demouser**
 - b. Password : **demo@pass123**

Click **Sign in**.

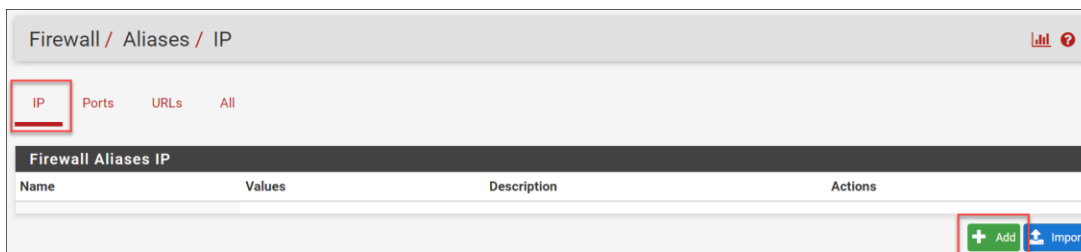


3. Click on **Firewall** followed by **Aliases**.



Aliases allow you to define a name that references one or more IP addresses. Using aliases simplifies NAT and Firewall rule creation.

4. On the **Firewall: Aliases** page, and while focused on the **IP** tab, click **Add** to add an IP alias.



5. On the **Firewall: Aliases: Edit** page enter the following:
 - a. Name: **WGMGMT1**

- b. Description: **WG Management Station**
- c. Type: **Host(s)**

In the **Host(s)** section, enter the Private IP address for the management server (10.7.0.12), and a description. Click **Save**. See the following screen shot for more details.

The screenshot shows the 'Firewall / Aliases / Edit' interface. Under the 'Properties' section, the 'Name' field contains 'WGMGMT1' (marked with a red circle 1), the 'Description' field contains 'WG Management Station' (marked with a red circle 2), and the 'Type' dropdown is set to 'Host(s)'. Under the 'Host(s)' section, the 'IP or FQDN' field contains '10.7.0.12' (marked with a red circle 3) and a description field contains 'WG Management Station' (marked with a red circle 4). At the bottom, there are 'Save' (marked with a red circle 5) and 'Add Host' buttons.

6. Complete steps 4 and 5 to add the following Aliases:

Name	Description	Type	IP	Description
WGSQ11	Woodgrove SQL Server	Host(s)	10.7.2.4	Woodgrove SQL Server
WGWEB1	WG Web Server 1	Host(s)	10.7.1.4	WG Web Server 1
WGWEB2	WG Web Server 2	Host(s)	10.7.1.5	WG Web Server 2
WGWEBLB	Internal Web Tier Load balancer	Host(s)	10.7.1.10	Internal Web Tier Load balancer
WGWEBSRVS	Woodgrove Web Servers	Host(s)	WGWEB1 WGWEB2	Woodgrove Web Servers

Note: The last alias (**bolded**) uses previously created aliases instead of IP addresses.

The creation screen of the last alias should look like the below:

Firewall / Aliases / Edit

Properties

Name

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description

A description may be entered here for administrative reference (not parsed).

Type

Host(s)

Hint Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

This button allows adding the 2nd host in this alias

Upon completion, your aliases should look like this:

Firewall / Aliases / IP

The alias list has been changed.
The changes must be applied for them to take effect.

IP Ports URLs All

Firewall Aliases IP

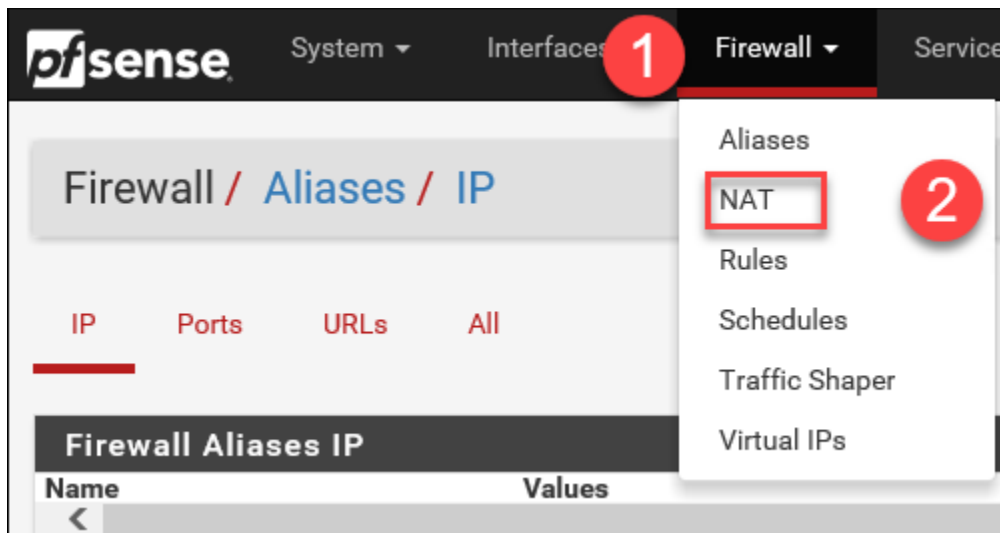
Name	Values	Description	Actions
WGMGMT1	10.7.0.12	WG Management Station	
WGSQ1	10.7.2.4	Woodgrove SQL Server	
WGWEB1	10.7.1.4	WG Web Server 1	
WGWEB2	10.7.1.5	WG Web Server 2	
WGWE1B	10.7.1.10	Internal Web Tier Load balancer	
WGWEBSRVS	WGWEB1, WGWEB2	Woodgrove Web Servers	

7. When all of the aliases are added, click **Apply changes**.

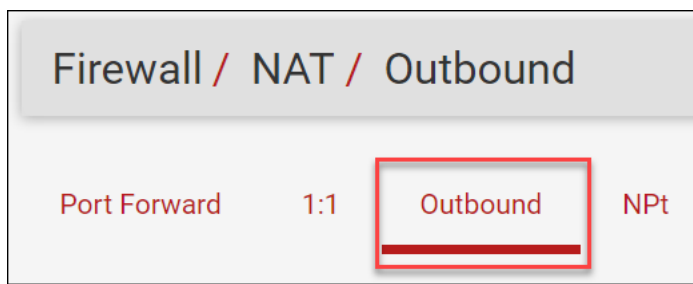


Task 2: Add NAT rules

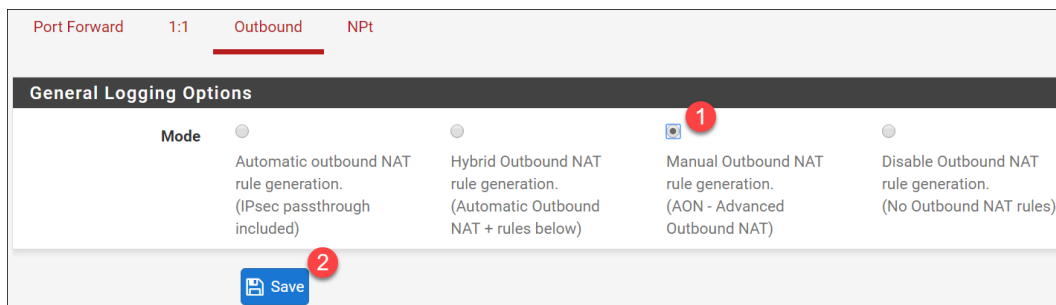
1. From the pfSense dashboard, click on **Firewall** and **NAT**.



2. Click on the **Outbound** tab.



3. Change the **Mode** from **Automatic outbound NAT rule generation** to **Manual outbound NAT rule generation**. Click **Save**.



4. In the **Mappings** section, click the **Add** button to add an outbound NAT rule.

Mappings										
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	WAN	127.0.0.0/8	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP - localhost to WAN	
<input type="checkbox"/>	WAN	127.0.0.0/8	*	*	*	WAN address	*	✗	Auto created rule - localhost to WAN	

↑ Add
↓ Add
🗑 Delete
💾 Save

5. On the **Firewall: NAT: Outbound: Edit** screen, enter the following:

- a. Source: **Network**
- b. Address: **10.7.0.0/16**

In the **Description** section, enter **Outbound to Internet**. Click **Save**.

Firewall / NAT / Outbound / Edit

Edit Advanced Outbound NAT Entry

Disabled Disable this rule

Do not NAT Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol any
Choose which protocol this rule should match. In most cases "any" is specified.

Source Network 10.7.0.0 / 16
Type Source network for the outbound NAT mapping. Port

Destination Any / 24
Type Destination network for the outbound NAT mapping. Port

Not
Invert the sense of the destination match.

Translation

Address Interface Address

Port Static port
Enter the source port or range for the outbound NAT mapping.

Misc

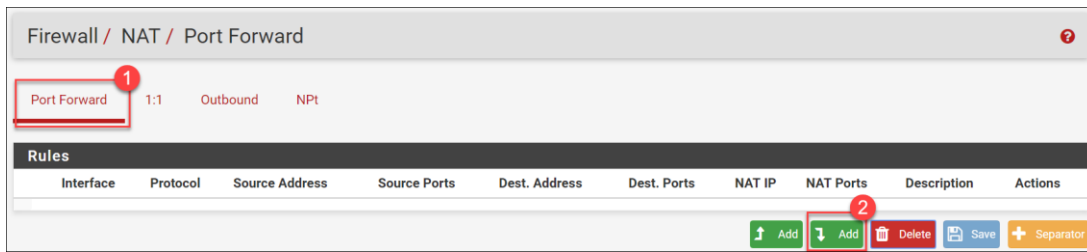
No XMLRPC Sync Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten.

Description Outbound to Internet
A description may be entered here for administrative reference (not parsed).

6. Click **Apply changes**.

The NAT configuration has been changed.
The changes must be applied for them to take effect.

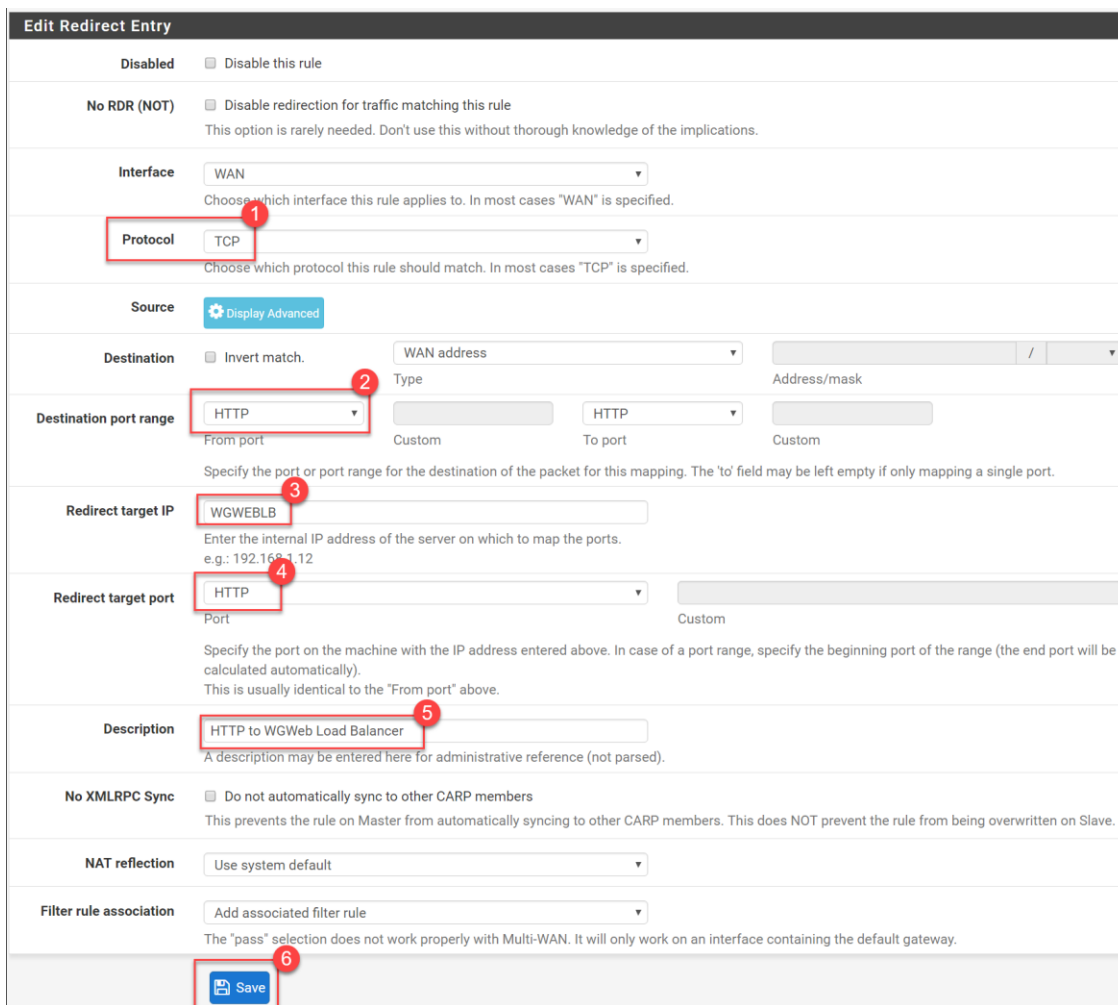
7. Click on the **Port Forward** tab, and click the **Add** to add a port forward rule.



8. In the **Firewall: NAT: Port Forward: Edit** screen make the following changes:

- a. Protocol: **TCP**
- b. Destination port range: drop-down **from** and choose **HTTP**
- c. Redirect target IP: **WGWEBLB**
- d. Redirect target port: from drop-down choose **HTTP**
- e. Description: **HTTP to WGWeb Load Balancer**

The remaining sections are correct. Click **Save**.



9. Create another NAT rule by repeating steps 7 and 8 using the following information:

- a. Protocol: **TCP/UDP**
- b. Destination port range: Manually enter **3445** in the **from** section
- c. Redirect target IP: **WGMGMT1**

- d. Redirect target port: From dropdown select **MS RDP**
- e. Description: **RDP to MGMT server**

The remaining sections are correct. Click **Save**.

Edit Redirect Entry

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol TCP/UDP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination Invert match. WAN address
Type: Address/mask

Destination port range Other 3445 Other
From port Custom To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP WGMGMT1
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12

Redirect target port MS RDP
Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description RDP to MGMT server
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Add associated filter rule
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

Save

10. Click **Apply changes**.

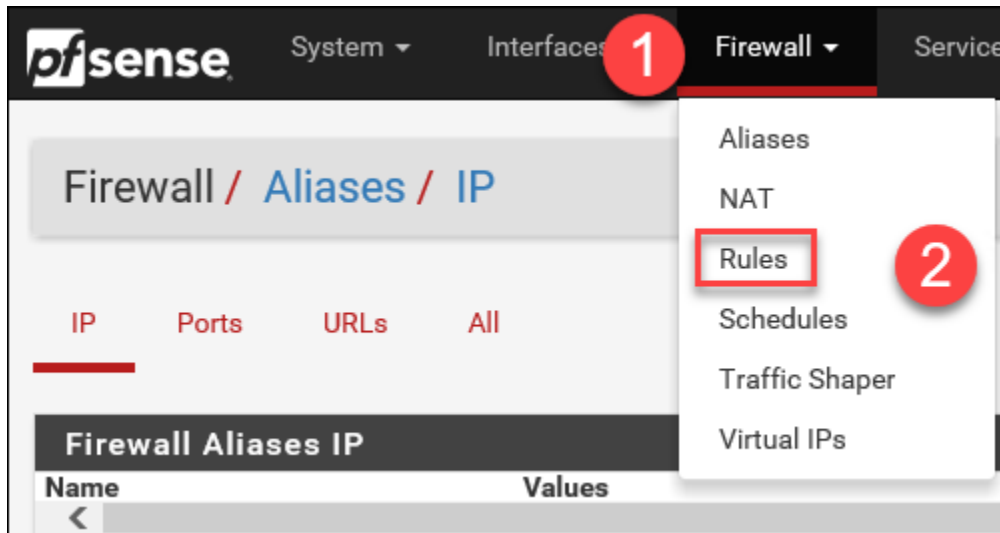
The NAT configuration has been changed.
The changes must be applied for them to take effect.

[Apply Changes](#)

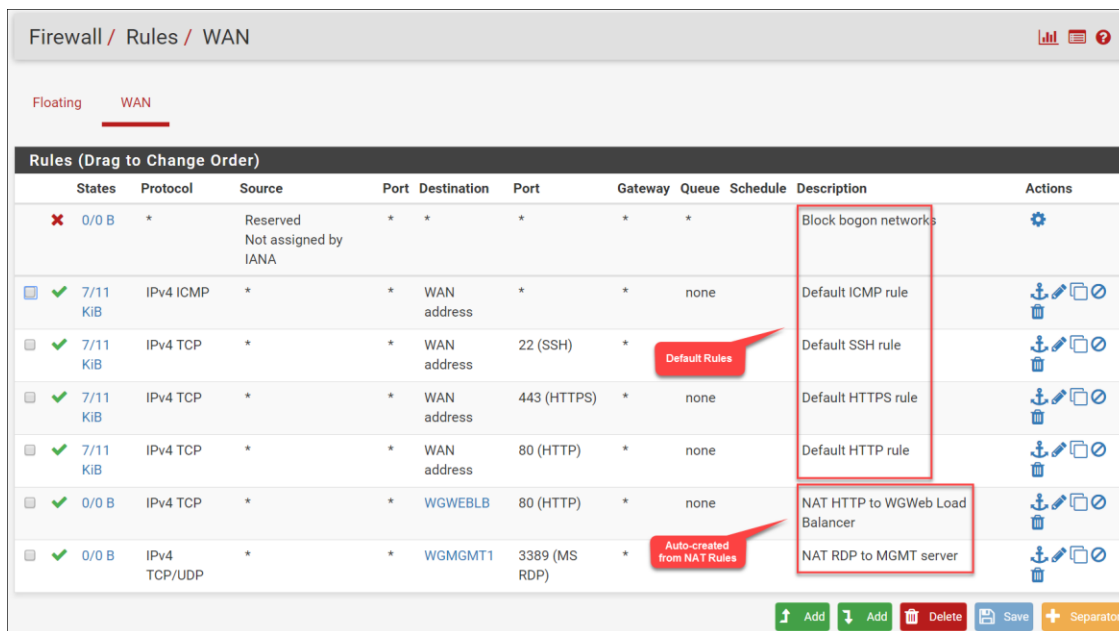
Task 3: Configure firewall rules

We have aliases and NAT rules configured. Now, we will create the firewall rules that will allow or block traffic.

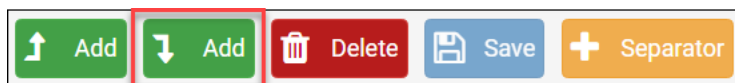
1. Click **Firewall**, and then click **Rules**.



2. Note that several rules already exist. Some are **default** rules (note the description field), and the last two rules were added automatically based on the NAT rules we configured.



3. Add a rule that will allow the management UI of the firewall to respond on a different port. At the bottom-right of the list of rules, click on **Add** to add a rule.



4. Enter the following information to define the new rule:
 - a. Destination: From dropdown menu, choose **WAN address**.

- b. Destination port range: Enter **8443** in the **from** box.
- c. Description: **MGMT HTTPS rule**
- d. Click **Save**.

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: TCP

Choose which IP protocol this rule should match.

Source

Source: Invert match. any

Source Address: /

Display Advanced:

Destination

Destination: Invert match. WAN address

Destination Address: /

Destination port range: (other) 8443 (other)

From: Custom To: Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: MGMT HTTPS rule

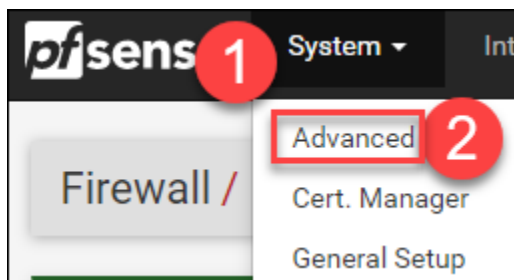
A description may be entered here for administrative reference.

Advanced Options:

- 5. Click **Apply changes**.

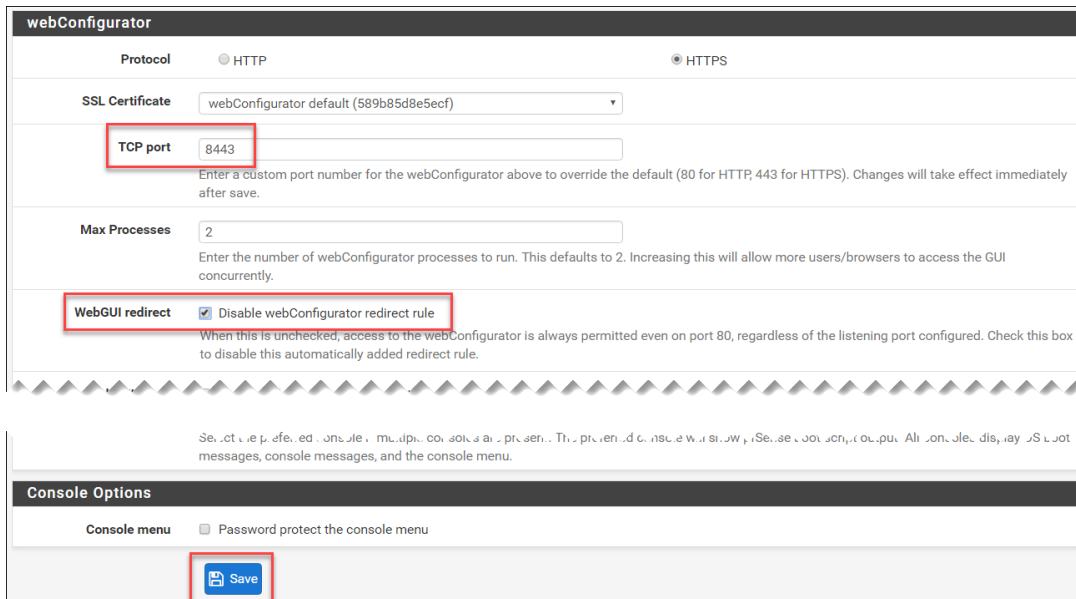


- 6. Click on **System**, followed by **Advanced**.

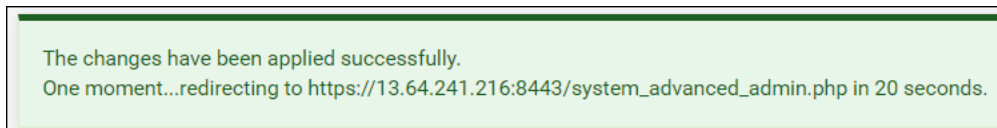


- 7. Under **webConfigurator**, make the following changes:

- a. Locate **TCP port**. In the box beside this field, enter **8443**.
- b. Locate **WebGUI redirect**, and check the box beside **Disable webConfigurator redirect rule**.
- c. Scroll down to the bottom of the page, and click **Save**.



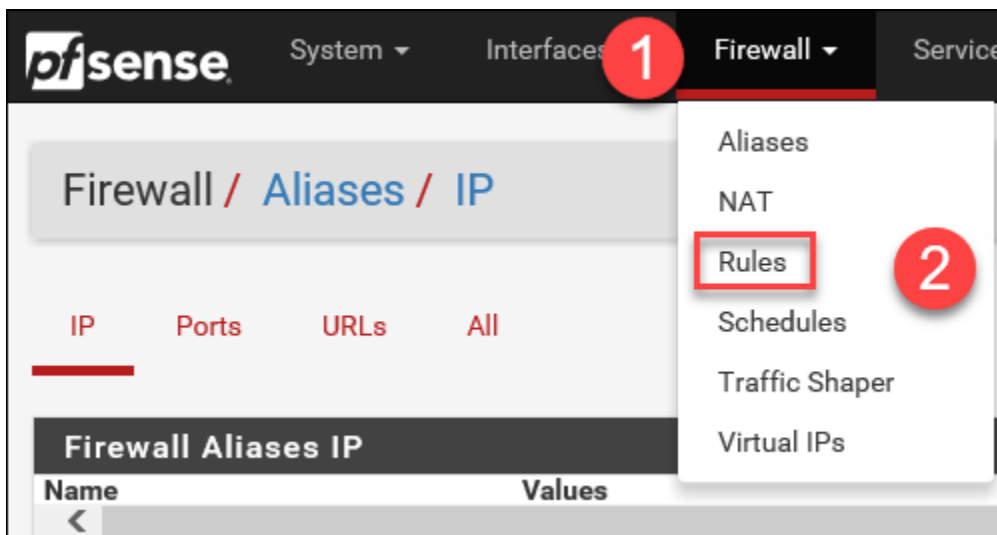
8. A prompt will appear notifying that webConfigurator will restart using the new management port:



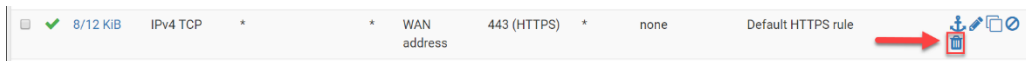
After the webConfigurator refreshes using the new port, proceed to the next step.

If it does not refresh properly, wait approximately 1 minute, and enter the port after the Public IP address in your browser. For example, if your Public IP address is 1.2.3.4, the URL should be: <https://1.2.3.4:8443>.

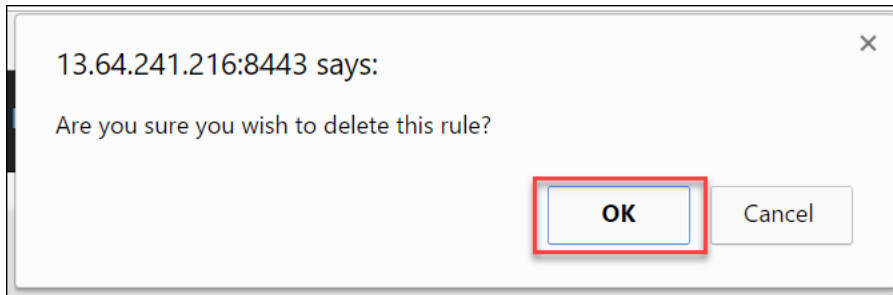
9. Click **Firewall** followed by **Rules**.



10. Locate a rule with the description "**Default HTTPS rule.**" Click the **trashcan icon** to delete it.



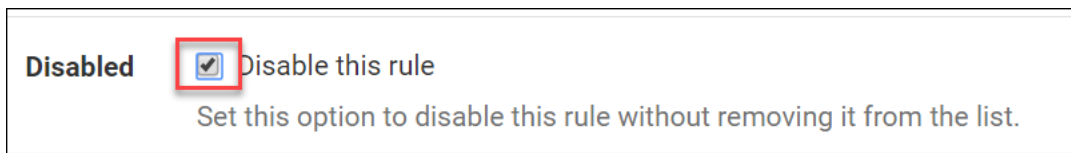
You will be prompted to confirm. Click **OK** to delete the rule.



11. Locate a rule with the description "**Default SSH rule.**" Click on the pencil icon to edit this rule.

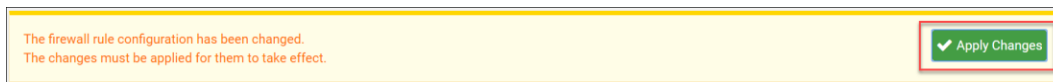


12. In the section called **Disabled**, check the box beside **Disable this rule**. Click **Save** at the bottom of the page.



Note: We disable this rule, as it is a favorite vector for attack. If we need to SSH into the firewall, we can enable here, do the required work, and disable it again.

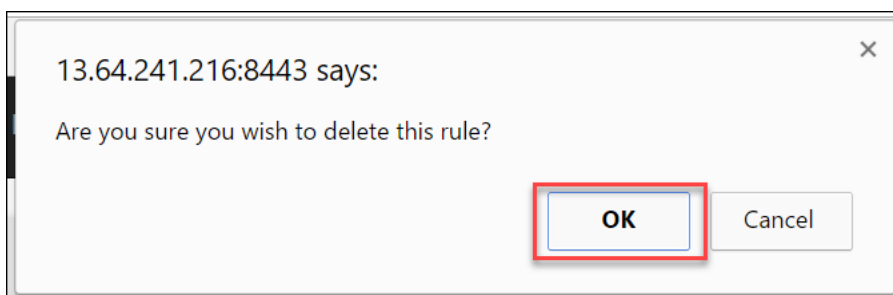
13. Click **Apply changes**.



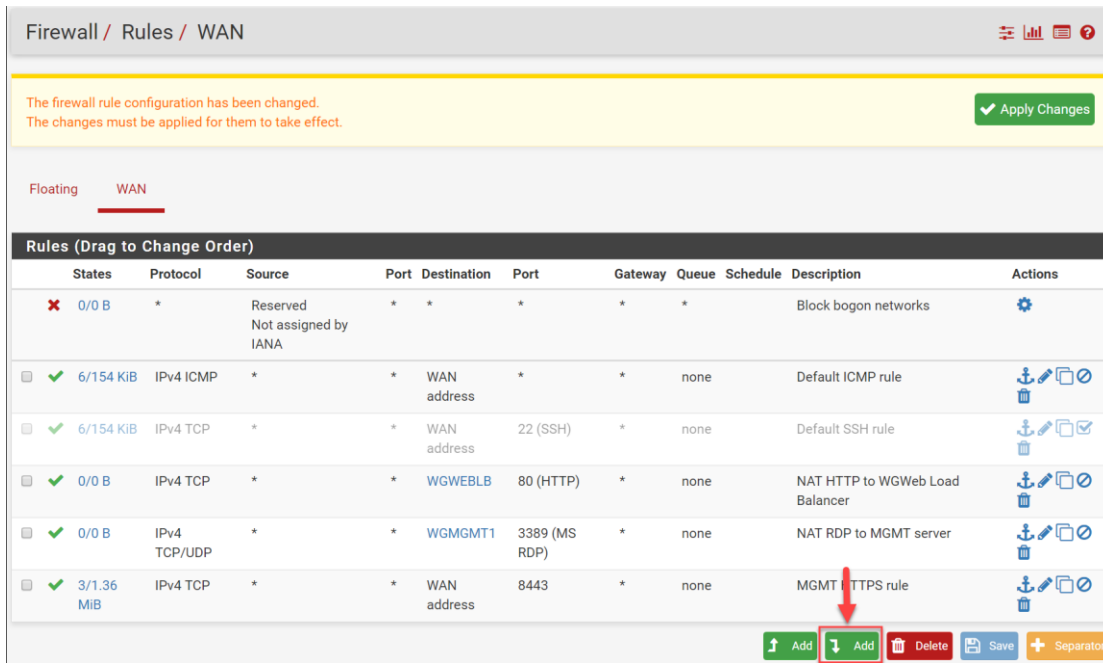
14. Locate a rule with the description "**Default HTTP rule.**" Click on the **trashcan icon** to delete this rule.



You will be prompted to confirm. Click **OK** to delete the rule.



15. On the **Firewall: Rules: WAN** page and underneath the rules and to the right, click on **Add** to add a new rule.



16. On the **Firewall: Rules: Edit** page make the following changes, and click **Save**.
 - a. Source: Drop-down **Type**, and choose **Network**. In the **Address** box, enter **10.7.0.0/16**
 - b. Destination port range: in 'from:' choose **HTTP** from dropdown menu
 - c. Description: **VNet to Any (HTTP)**
 - d. At the bottom, click **Save**.

Firewall / Rules / Edit

Edit Firewall Rule

Action
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface
 Choose the interface from which packets must come to match this rule.

Address Family
 Select the Internet Protocol version this rule applies to.

Protocol
 Choose which IP protocol this rule should match.

Source

Source Invert match. /
 Display Advanced

Destination

Destination Invert match. /
Destination port range
 From Custom To Custom
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
 A description may be entered here for administrative reference.

Advanced Options

17. Repeat steps 15 and 16 to create an additional rule using the following information:
 - a. Protocol: **TCP**
 - b. Source:
 - i. Type: **Network**
 - ii. Address: **10.7.0.0/16**
 - c. Destination port range:
 - i. From: Choose **HTTPS** from the dropdown menu
 - d. Description: **VNet to Any (HTTPS)**
 - e. Click **Save** at the bottom.
18. Repeat steps 15 and 16 to create an additional rule using the following information:
 - a. Protocol: **TCP**
 - b. Source:
 - i. Type: **Single host or alias**
 - ii. Address: **WGWEBSRVS**
 - c. Destination:
 - i. Type: **Single host or alias**
 - ii. Address: **WGSQ1**
 - d. Destination port range:

- i. From: Type **1433** in the **Custom** box
- e. Description: **Allow Web Servers to SQL1 TCP1433**
- f. Click **Save** at the bottom.

The screenshot shows the 'Edit Firewall Rule' configuration page in Azure. The rule is named 'Allow Web Servers to SQL1 TCP1433'. The configuration is as follows:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** WAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Invert match. Single host or alias: WGWEBSRVS
- Destination:** Invert match. Single host or alias: WGSQ1
- Destination port range:** (other) 1433 (other) Custom
- Description:** Allow Web Servers to SQL1 TCP1433
- Log:** Log packets that are handled by this rule
- Advanced Options:** Display Advanced
- Save:**

19. Repeat steps 15 and 16 to create an additional rule using the following information:
 - a. Protocol: **TCP/UDP**
 - b. Source:
 - i. Type: **Single host or alias**
 - ii. Address: **WGMGMT1**
 - c. Destination:
 - i. Type: **Single host or alias**
 - ii. Address: **WGWEBSRVS**
 - d. Destination port range:
 - i. From: Choose **MS RDP** from drop-down
 - e. Description: **Allow RDP from MGMT to Web Servers**
 - f. Click **Save** at the bottom.

Firewall / Rules / Edit

Edit Firewall Rule

Action
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface
 Choose the interface from which packets must come to match this rule.

Address Family
 Select the Internet Protocol version this rule applies to.

Protocol
 Choose which IP protocol this rule should match.

Source

Source Invert match. /

Display Advanced

Destination

Destination Invert match. /

Destination port range
 From Custom To Custom
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
 A description may be entered here for administrative reference.

Advanced Options

20. Click **Apply changes**.

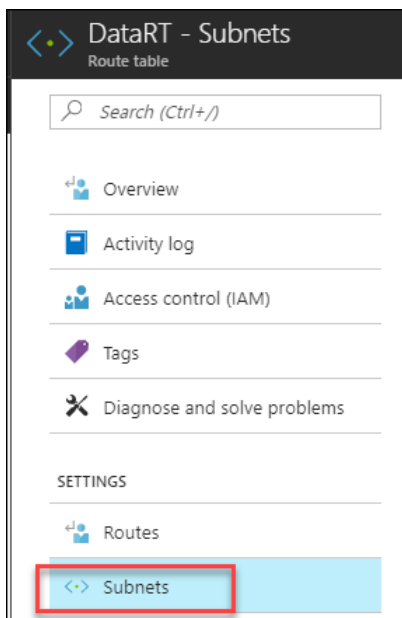
The firewall rule configuration has been changed.
 The changes must be applied for them to take effect.

21. Upon completion, your firewall rules should look like the following:

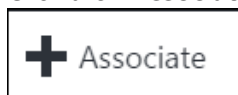
Floating		WAN		Rules (Drag to Change Order)							
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
✘ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	⚙️	
☑️ 7/217 KiB	IPv4 ICMP	*	*	WAN address	*	*	none		Default ICMP rule	📌 📄 🗑️	
☑️ 7/217 KiB	IPv4 TCP	*	*	WAN address	22 (SSH)	*	none		Default SSH rule	📌 📄 🗑️	
☑️ 0/0 B	IPv4 TCP	*	*	WGWEBLB	80 (HTTP)	*	none		NAT HTTP to WGWeb Load Balancer	📌 📄 🗑️	
☑️ 0/0 B	IPv4 TCP/UDP	*	*	WGMGMT1	3389 (MS RDP)	*	none		NAT RDP to MGMT server	📌 📄 🗑️	
☑️ 8/1.67 MiB	IPv4 TCP	*	*	WAN address	8443	*	none		MGMT HTTPS rule	📌 📄 🗑️	
☑️ 0/0 B	IPv4 TCP	10.7.0.0/16	*	*	80 (HTTP)	*	none		VNet to Any (HTTP)	📌 📄 🗑️	
☑️ 0/0 B	IPv4 TCP	10.7.0.0/16	*	*	443 (HTTPS)	*	none		VNet to Any (HTTPS)	📌 📄 🗑️	
☑️ 0/0 B	IPv4 TCP	WGWEBSRVS	*	WGSQ1	1433	*	none		Allow Web Servers to SQL1 TCP1433	📌 📄 🗑️	
☑️ 0/0 B	IPv4 TCP/UDP	WGMGMT1	*	WGWEBSRVS	3389 (MS RDP)	*	none		Allow RDP from MGMT to Web Servers	📌 📄 🗑️	

Task 4: Associate route tables to subnets

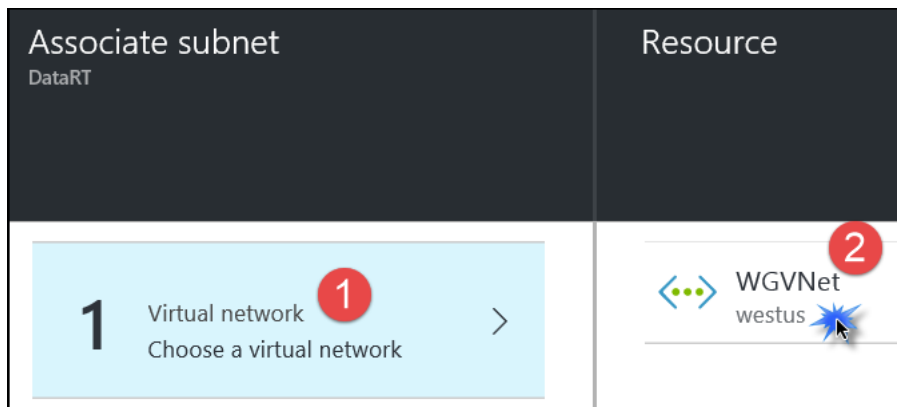
- Using the Azure portal, open the WGVNetRG resource group.
- Click on **DataRT**, followed by **Subnets**.



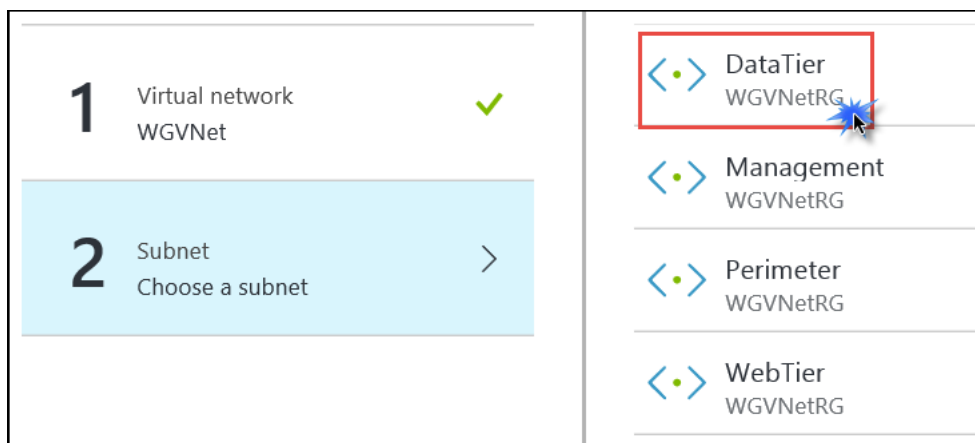
- Click the **+Associate**.



- On the **Associate subnet** blade, click on **Virtual network**. Then, click on **WGVNet**.



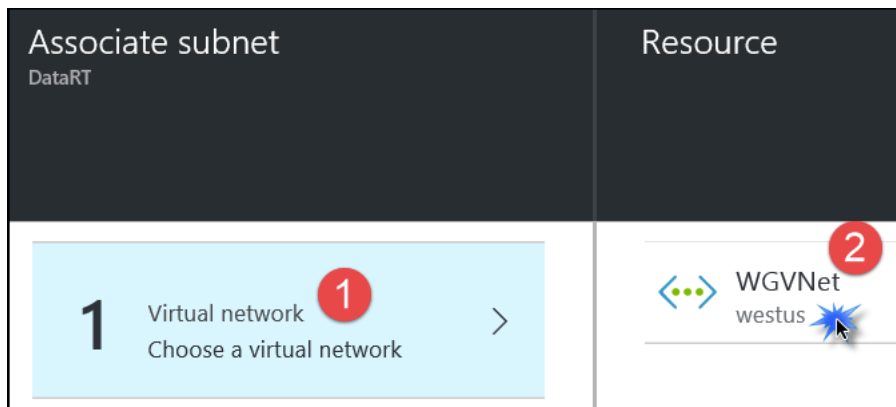
5. From the **Choose a subnet** blade, click on **DataTier**.



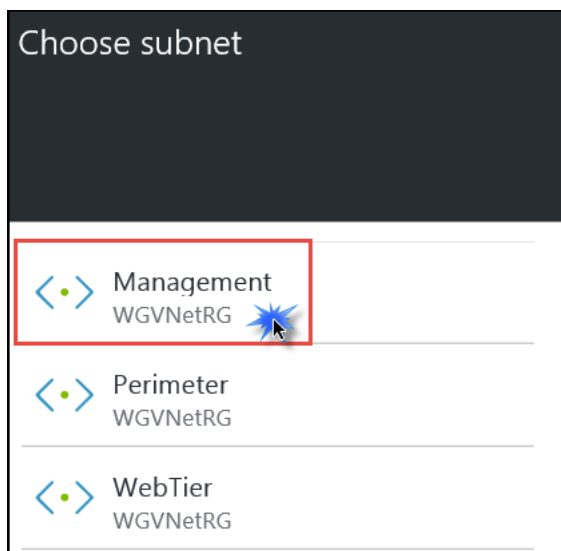
6. Click **OK** at the bottom of the **Associate subnet** blade.
7. Move back to the resource group, and click on **MgmtRT**, then **Subnets**.
8. Click the **+Associate**.



9. On the **Associate subnet** blade, click on **Virtual network**. Click on **WGVNet**.



10. The **Choose subnet** blade opens. Click on **Management**.



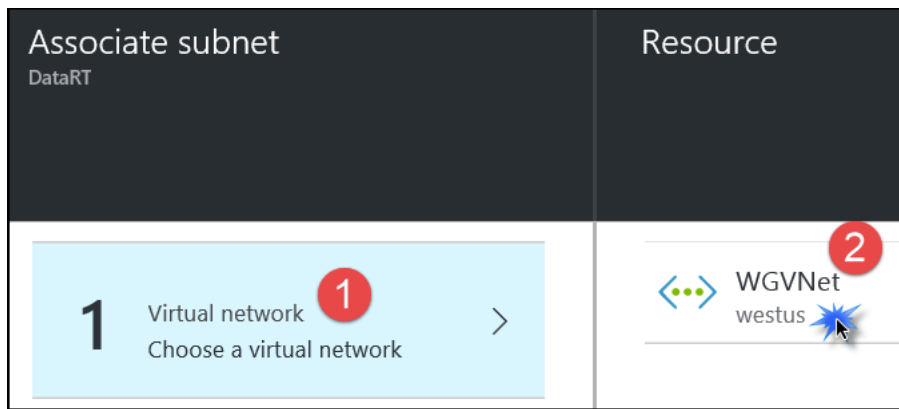
11. Click **OK** at the bottom of the **Associate subnet** blade.

12. Back on the resource group click on **WebRT** followed by **Subnets**.

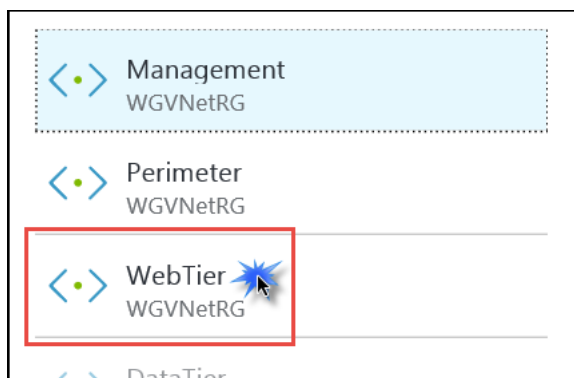
13. Click the **+Associate**.



14. On the **Associate subnet** blade, click on **Virtual network**. Then, click on **WGVNet**.



15. The **Choose subnet** blade opens. Click on **WebTier**.



16. Click **OK** at the bottom of the **Associate subnet** blade.

Task 5: Validate connectivity

Now it is time to validate the configuration steps have resulted in the following connectivity:

- RDP from the Internet to the **WGMGMT1** server using the firewall's Public IP address and port 3445
- While RDPed into the MGMT server, RDP to either of the WEB servers
- Browse the CloudShop web application from the Internet using the firewall's Public IP address and port 80.

RDP to WGMGMT1 server and from MGMT to WEB server

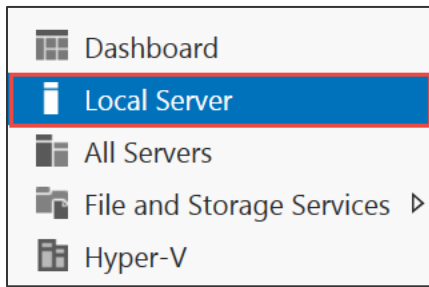
1. Click the Windows button and type in **mstsc**, and hit the **enter** key. This should open the Remote Desktop client.
2. In the **Computer** section, enter **<firewall public IP>:3445**, for example, **13.65.88.31:3445**
3. When prompted, enter the credentials:
 - a. User: **demouser**
 - b. Password: **demo@pass123**
4. At the security certificate warning, click **Yes** to connect.



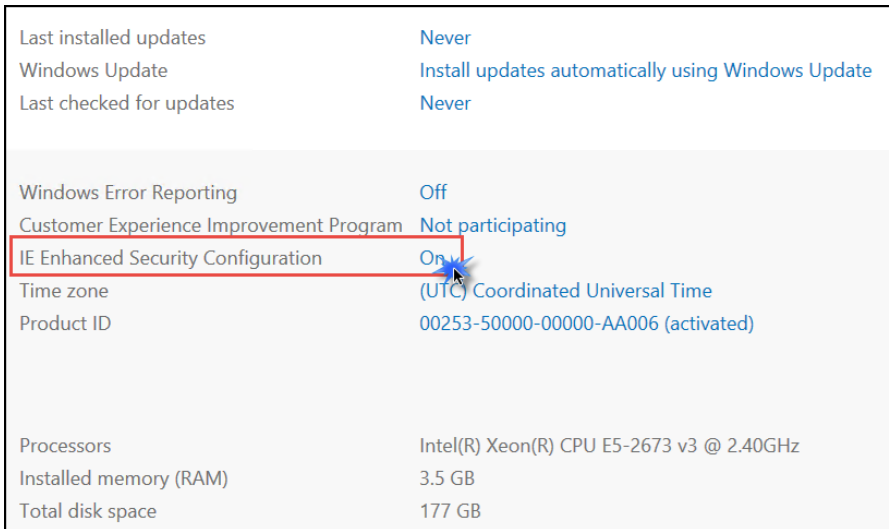
5. You should see the desktop of WGMGMT1 in a few seconds.
6. From within the RDP session, click on the Windows button of WGMGMT1 and type in **mstsc** and hit the **enter** key.
7. In the **Computer** section enter the Private IP address of WGWEB1 (10.7.1.4), and click **Connect**.
8. When prompted, enter the credentials:
 - a. User: **demouser**
 - b. Password: **demo@pass123**
9. At the security certificate warning, click **Yes** to connect.
10. Connectivity is validated when you see the desktop of WGWEB1. Disconnect the RDP session to WGWEB1 (10.7.1.4).

Validate internal connectivity to CloudShop

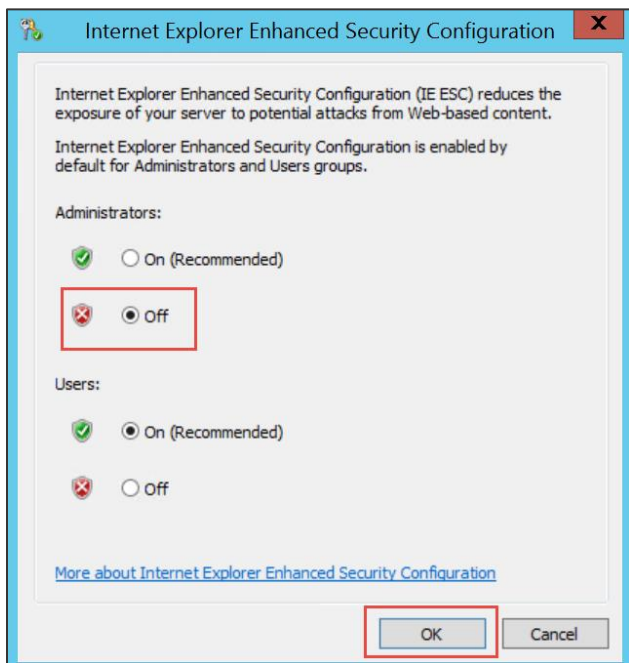
1. While still RDPed into WGMGMT1, open **Server Manager** (if it is not already opened).
2. On the left, click **Local Server**.



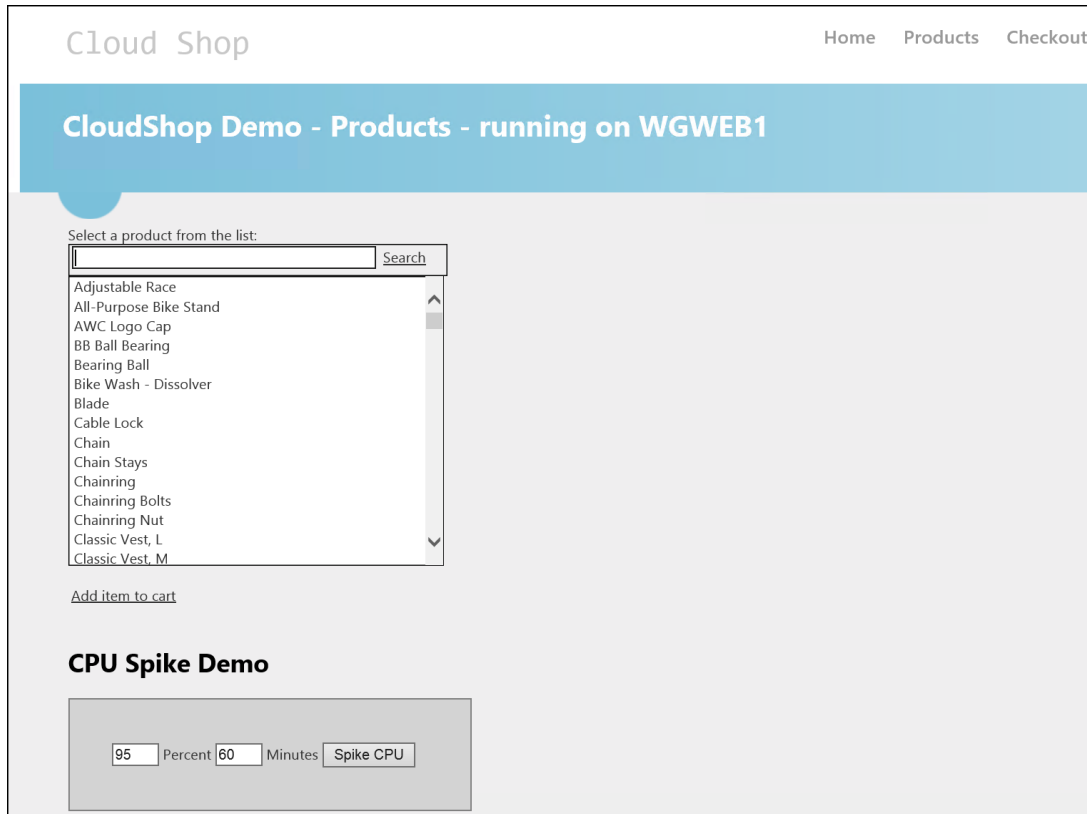
3. On the right side of the pane, click **On** by **IE Enhanced Security Configuration**.



4. Change to **Off** for Administrators, and click **OK**.



5. Open Internet Explorer, enter the IP address of WGWEB1 (10.7.1.4) in the URL section, and press the **Enter** key. You should see the CloudShop application.



6. Now, enter the IP address of the load balancer (10.7.1.10), and validate you can access CloudShop. After validation, close the RDP session to WGMGMT1.
7. Open a browser on your client machine, and enter <http://<firewall public IP>>, for example, <http://13.65.88.31>.
8. Validate you see the CloudShop website returned. If you refresh the page several times, you should notice both WEB servers being accessed.

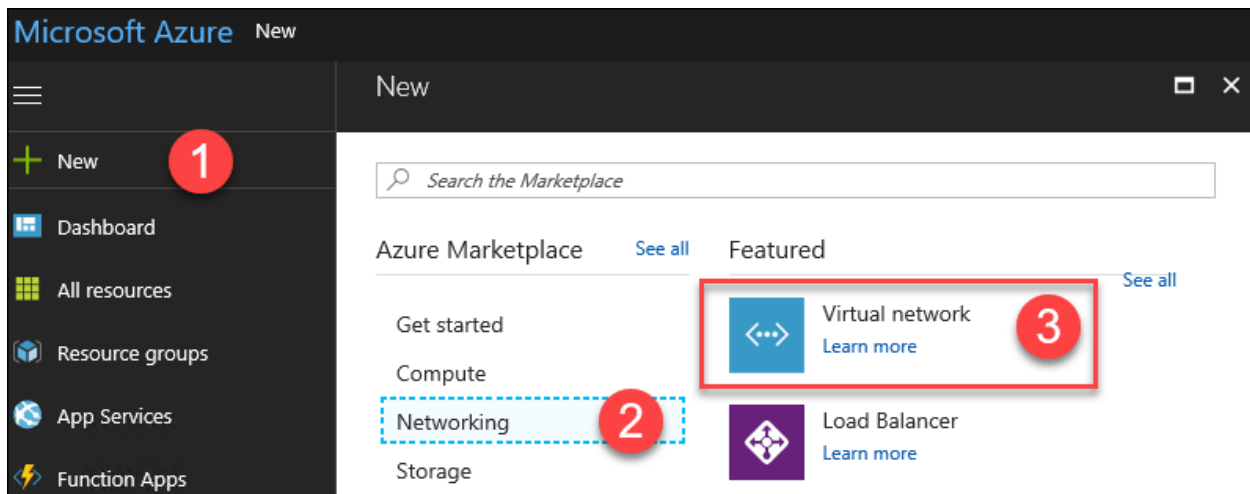
Exercise 7: Configure site-to-site connectivity

Duration: 60 minutes

In this exercise, we will simulate an on-premises connection to the internal web application. To do this, we will first set up another virtual network in a separate Azure region followed by the site-to-site connection of the 2 virtual networks. Finally, we will set up a virtual machine in the new virtual network to simulate on-premises connectivity to the internal load-balancer.

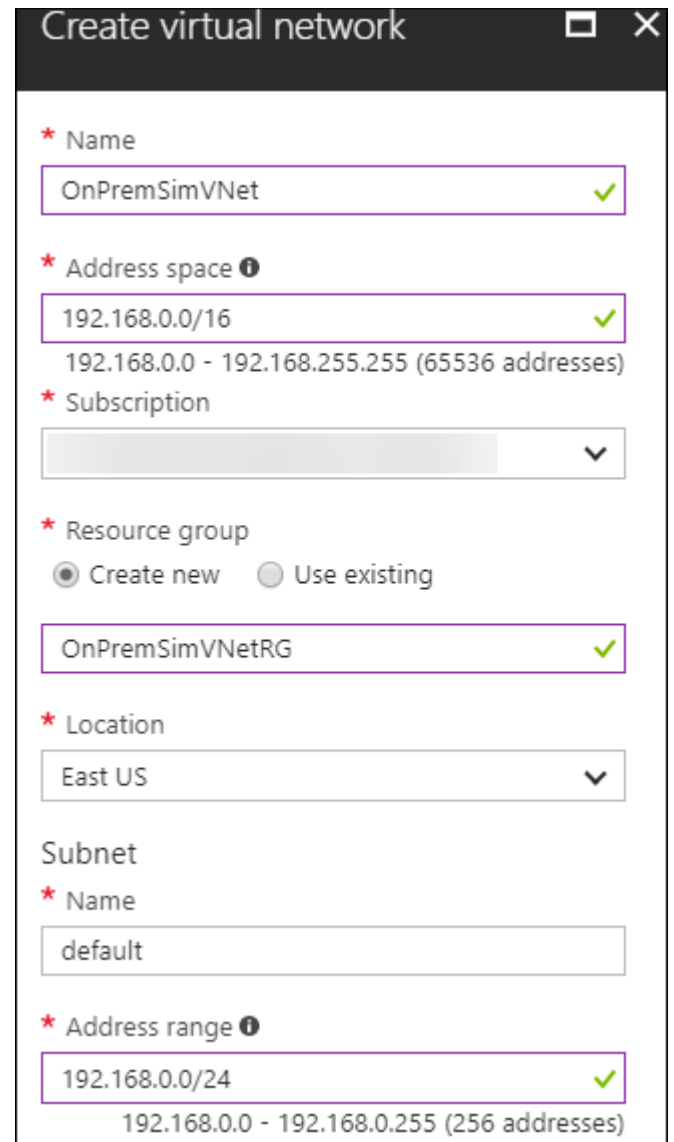
Task 1: Create another virtual network

1. Using the Azure Management portal, click **New**, **Networking**, and **Virtual network**.



2. See the following screenshot, and specify the configuration:

- Name: **OnPremSimVNet**
 - Address space: **192.168.0.0/16**
 - Subscription: **Choose your Subscription**
 - Resource Group: Create new:
OnPremSimVNetRG
 - Subnet name: **default**
 - Subnet address range: **192.168.0.0/24**
 - Location: **East US**
- Make sure this is **not** the same location you have specified in the previous labs.



Create virtual network

* Name
OnPremSimVNet ✓

* Address space ⓘ
192.168.0.0/16 ✓
192.168.0.0 - 192.168.255.255 (65536 addresses)

* Subscription
▼

* Resource group
 Create new Use existing

OnPremSimVNetRG ✓

* Location
East US ▼

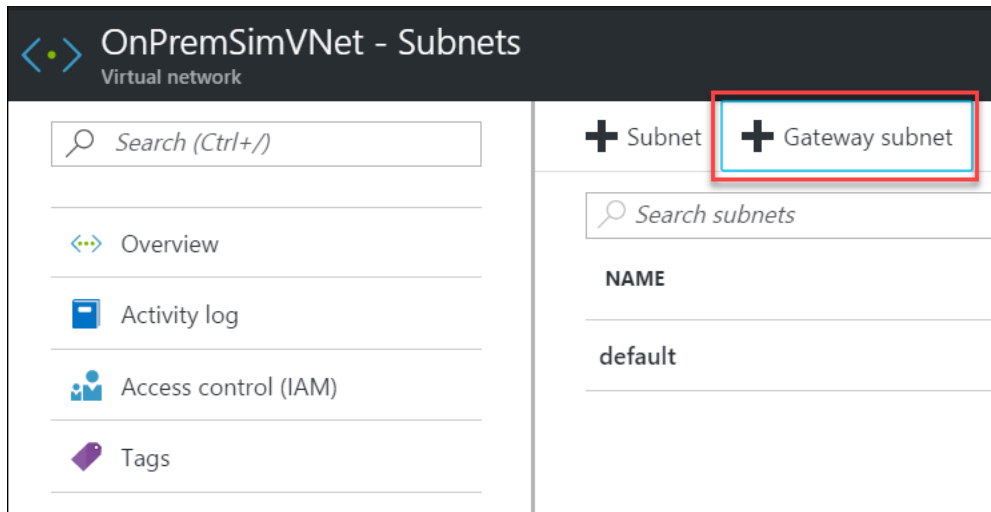
Subnet

* Name
default

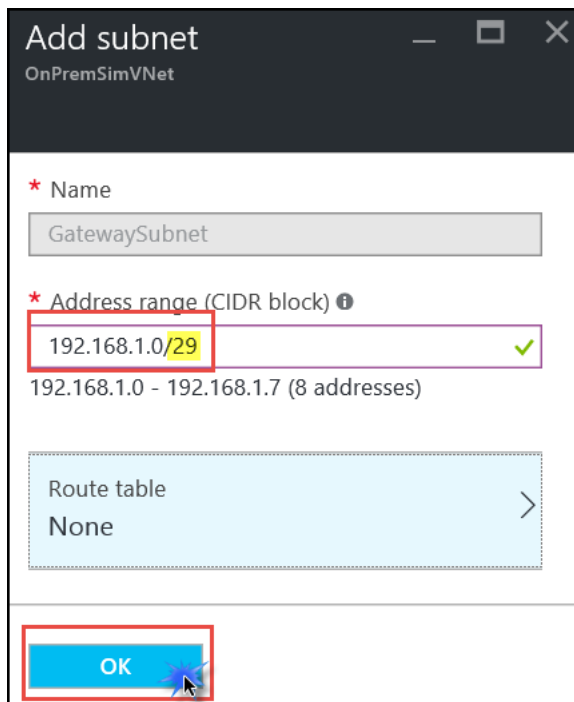
* Address range ⓘ
192.168.0.0/24 ✓
192.168.0.0 - 192.168.0.255 (256 addresses)

Task 2: Configure gateway subnets for both virtual networks

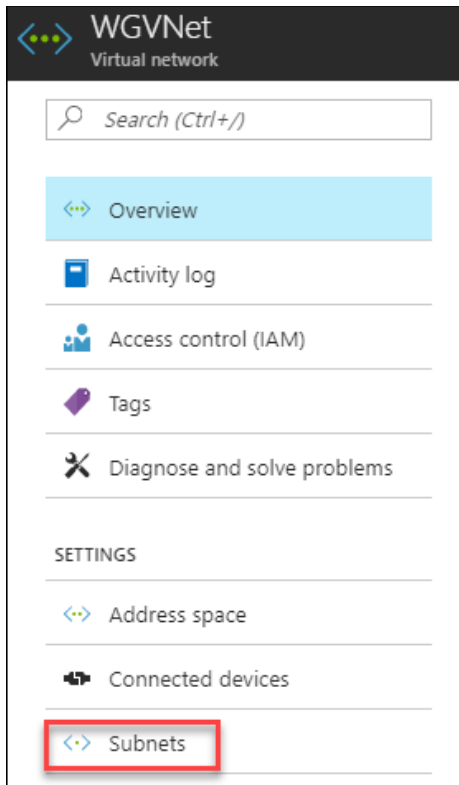
1. Open the **OnPremSimVNet** blade, and click **Subnets**.
2. Next, click +**Gateway subnet**.



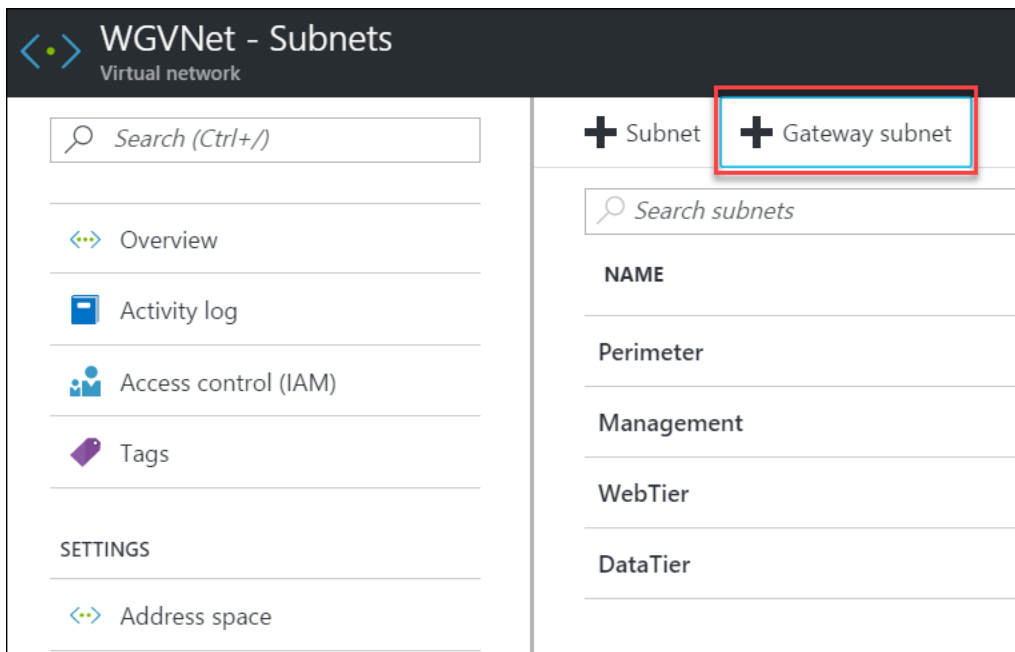
- Specify the following configuration for the subnet, and click **OK**.
 - Address range: **192.168.1.0/29**
 - Route table: **None** (we will add later)



- Next, you will add the gateway subnet to the **WGVNet** virtual network. First, open the **WGVNet** blade, and click Subnets.

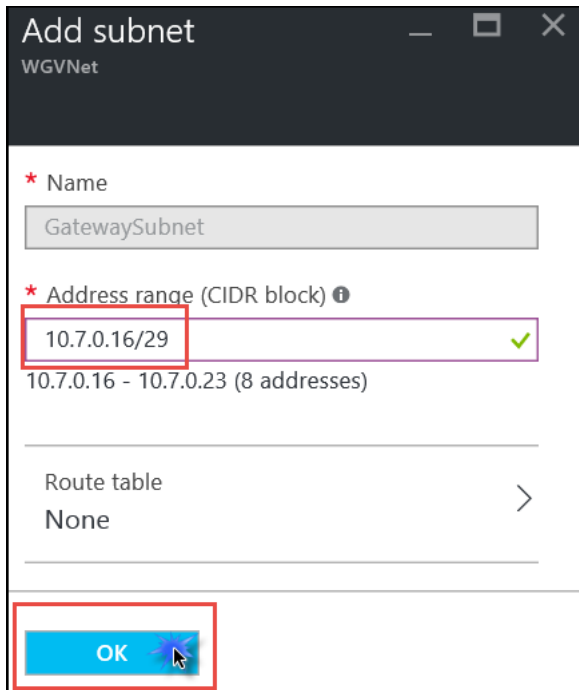


5. Click **+Gateway subnet**.



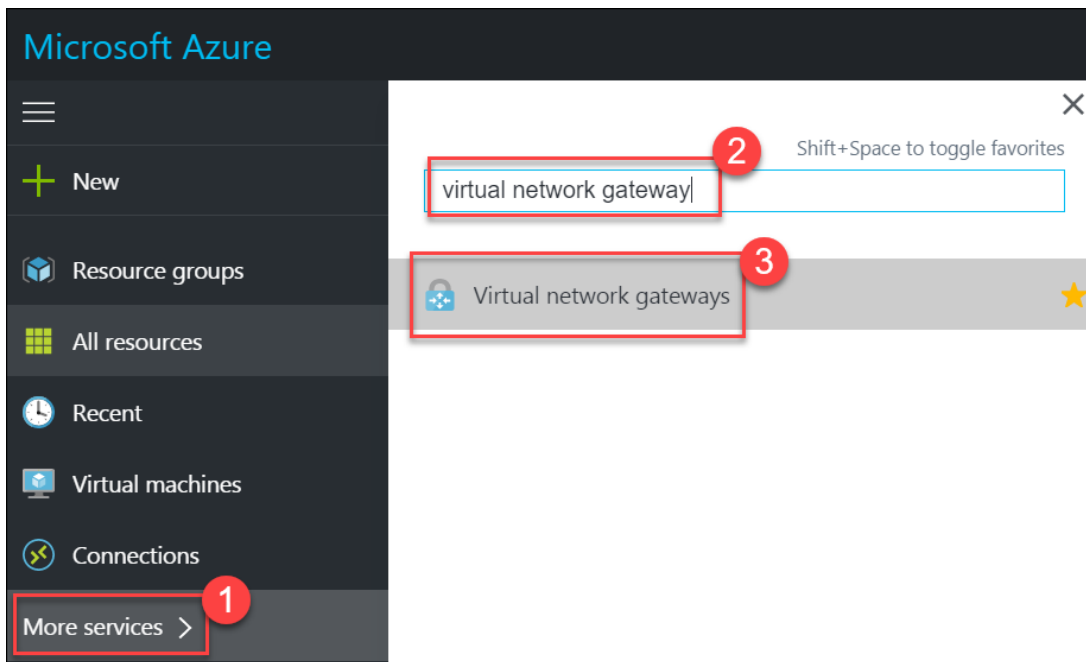
6. Specify the following configuration, and click **OK**.

- Address range: **10.7.0.16/29**
- Route table: **None**

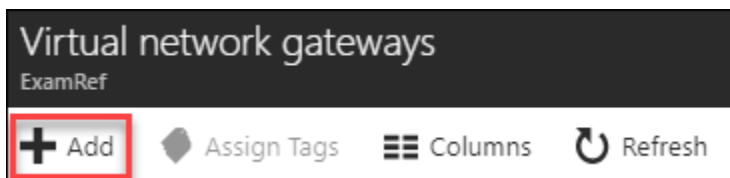


Task 3: Create the first gateway

- Using the Azure Management portal, click **More services**, type **virtual network gateway** in the search window, and click **Virtual Networks Gateways**.



- Click the **+Add** button on the toolbar.



- Name the gateway **AzureWGGW**.

- One of the last configurable options is the **Location**. Click to choose the Azure region where **WGVNet** exists (West US if following this guide).

- In the **Virtual network** section, click **Choose a virtual network**, and click **WGVNet**.

- Click the **Public IP address** tile, and click **Create new**.

- Name the IP **AzureWGGWPIP**, and click **OK**.

- Validate your settings look like the following screenshot, and then click **Create**.

Create virtual network gateway... ☐ ✕

* Name
AzureWGGW ✓

Gateway type ⓘ
VPN ExpressRoute

VPN type ⓘ
Route-based Policy-based

* SKU ⓘ
VpnGw1 ▼

Enable active-active mode ⓘ

* Virtual network ⓘ >
WGVNet

* First IP configuration >
(new) AzureWGGWPIP

Configure BGP ASN

* Subscription ▼

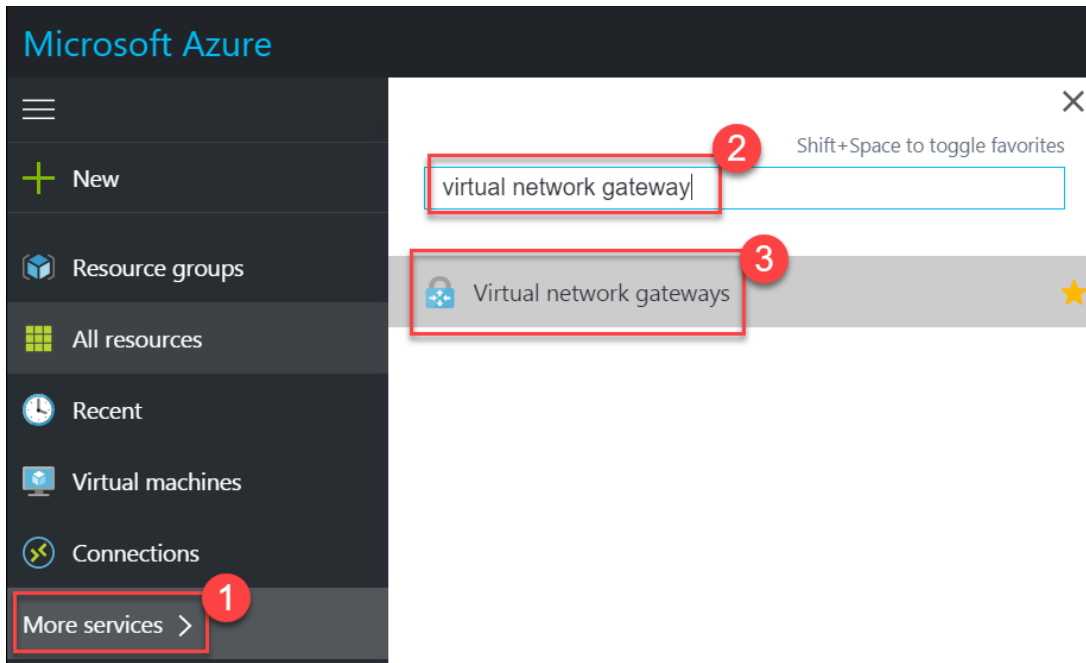
Resource group ⓘ
WGVNetRG

* Location ⓘ ▼
West US

NOTE: The gateway will take 30-45 minutes to provision. Continue to the next section while waiting.

Task 4: Create the second gateway

1. Using the Azure Management portal, click **More services**, type **virtual network gateway** in the search window, and click **Virtual Networks Gateways**.



2. Click the **Add** button on the toolbar.
3. Name the gateway **OnPremWGGW**.

* Name

OnPremWGGW ✓

4. One of the last configurable options is the **Location**. Click to choose the Azure region where **OnPremSimVNet** exists (East US if following this guide).

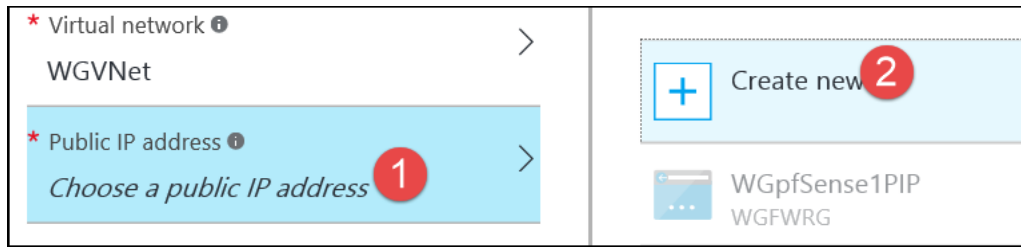
* Location ⓘ

East US ▼

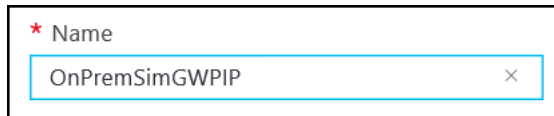
5. In the **Virtual network** section, click **Choose a virtual network** followed by **OnPremSimVNet**.

<p>* Name</p> <p>OnPremWGGW ✓</p> <p>* Virtual network ⓘ 1 ></p> <p><i>Choose a virtual network</i></p> <p>* Public IP address ⓘ ></p> <p><i>Choose a public IP address</i></p>	<p>i These are the virtual networks in the selected subscription and location 'East US'.</p> <hr/> <p><...> OnPremSimVNet 2</p> <p>OnPremSimVNetRG</p>
--	--

6. Click the **Public IP address** tile, and click **Create new**.



7. Name the IP **OnPremSimGWPIP**, and click **OK**.



8. Validate your settings look like the following screenshot, and click **Create**.

Create virtual network gateway...

* Name
OnPremWGGW ✓

Gateway type ⓘ
VPN ExpressRoute

VPN type ⓘ
Route-based Policy-based

* SKU ⓘ
VpnGw1 ▼

Enable active-active mode ⓘ

* Virtual network ⓘ >
OnPremSimVNet

* First IP configuration >
(new) OnPremWGGWPIP

Configure BGP ASN

* Subscription
▼

Resource group ⓘ
OnPremSimVNetRG

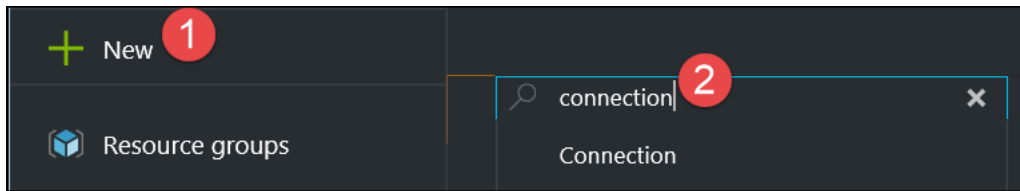
* Location ⓘ
East US ▼

Note: The gateway will take 30-45 minutes to provision. You will need to wait until both gateways are provisioned before proceeding to the next section.

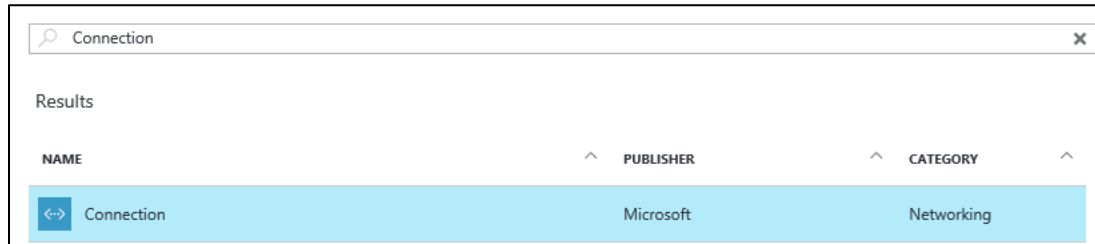
9. The Azure portal will notify you when the deployments have completed.

Task 5: Connect the gateways

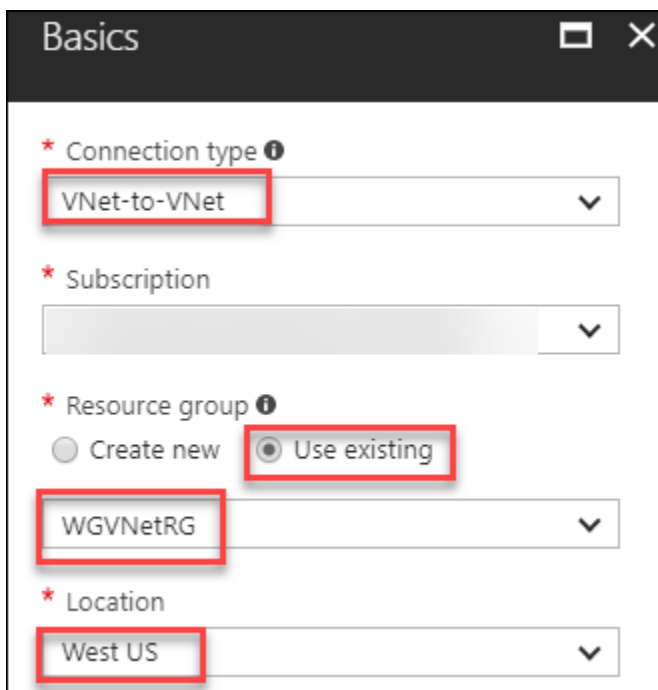
1. Using the Azure Management portal, click **New**, type in **Connection**, and press **Enter**.



2. Click **Connection**, and click **Create**.



3. On the **Basics** blade, leave the **Connection type** set to **VNet-to-VNet**. Select the existing **WGVMRG** resource group. Then, change the location of this connection to the Azure region the **WGVNet** virtual network is deployed to (West US). Click **OK**.

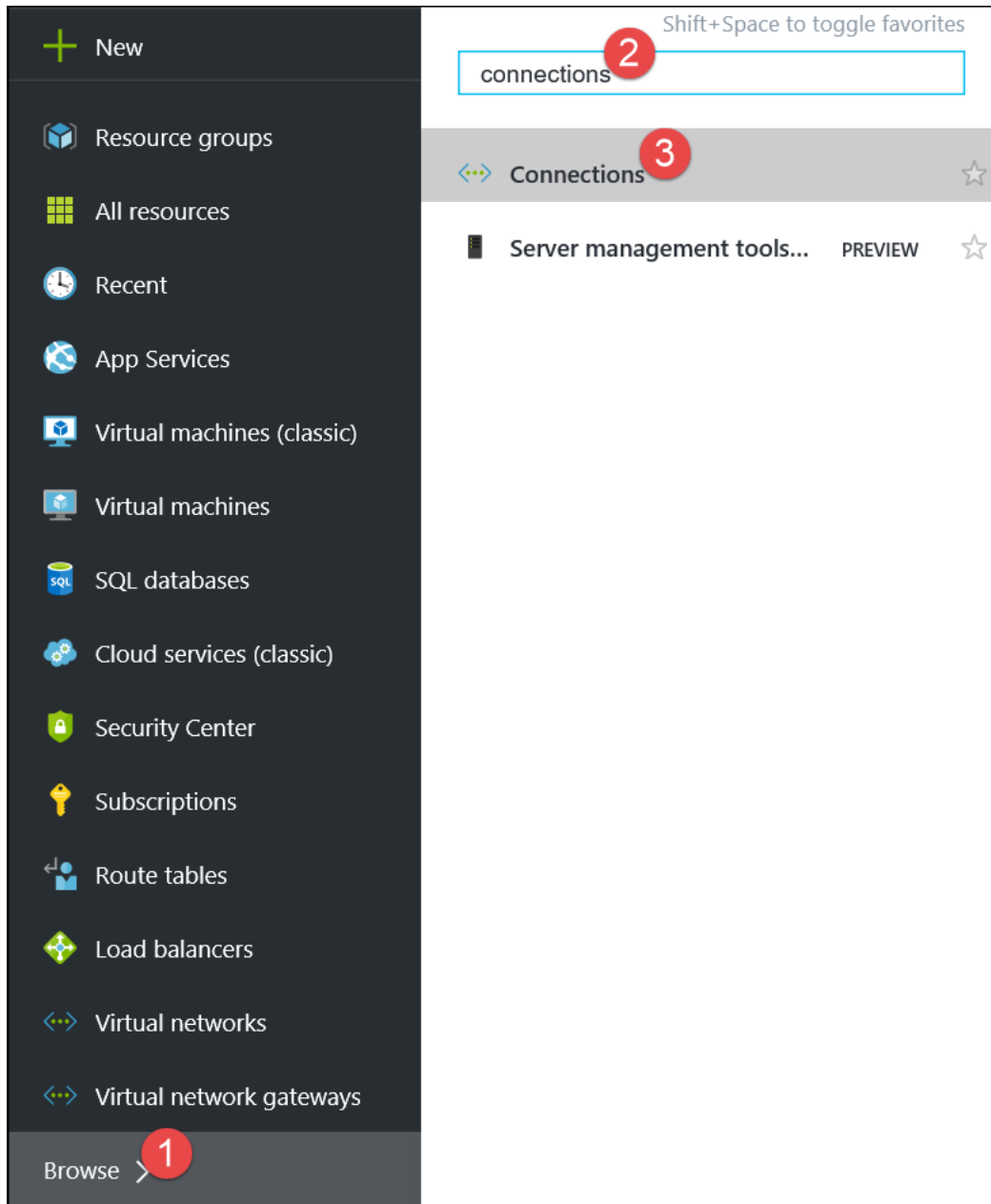


4. On the Settings tab, select **AzureWGGW** for the first virtual network gateway and **OnPremWGGW** for the second virtual network gateway. Ensure **Establish bidirectional connectivity** is selected. Enter a Shared key, such as **A1B2C3D4** for example. After your settings reflect the below screenshot, click **OK**.

The screenshot shows a configuration page for a virtual network gateway connection. It includes the following fields and options:

- * First virtual network gateway** (with an information icon): A dropdown menu showing "AzureWGGW".
- * Second virtual network gateway** (with an information icon): A dropdown menu showing "OnPremSimGW".
- Establish bidirectional connectivity** (with an information icon): A checked checkbox.
- * First connection name**: A text input field containing "AzureWGGW-to-OnPremSimGW" with a green checkmark on the right.
- * Second connection name**: A text input field containing "OnPremSimGW-to-AzureWGGW" with a green checkmark on the right.
- * Shared key (PSK)** (with an information icon): A text input field containing "A1B2C3D4" and a close button (X) on the right.

5. Click **OK** on the **Summary** page to create the connection.
6. Using the Azure Management portal, click **More services**. Then, type **connections** in the search window and select **Connections**.



7. Watch the progress of the connection status, and use the **Refresh** icon until the status changes for both connections from **Unknown** to **Connected**. This may take 5 minutes or more.

Connections

+ Add Columns Refresh

Subscriptions: Visual Studio Enterprise – Don't see a subscription? [Switch directories](#)

Filter items...

NAME	STATUS	PEER 1	PEER 2	RESOURCE GROUP	LOCATION
AzureWGGW-to-OnPremSimGW	Connected	AzureWGGW	OnPremSimGW	WGVMRG	West US
OnPremSimGW-to-AzureWGGW	Connected	OnPremSimGW	AzureWGGW	WGVMRG	East US

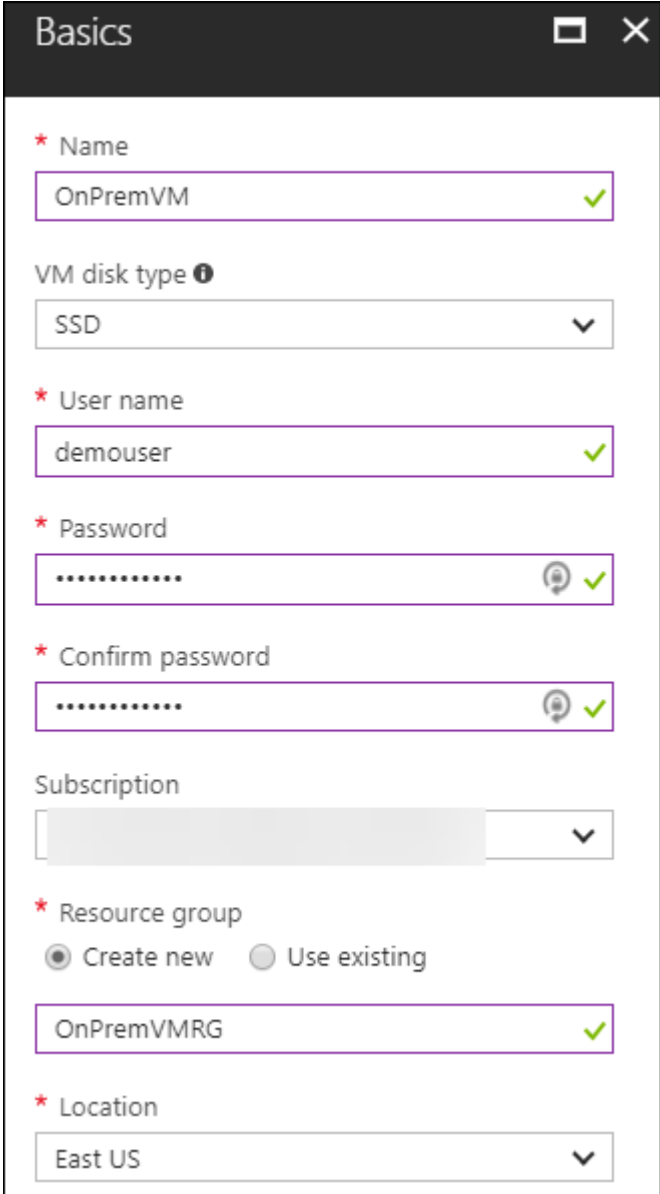
Exercise 8: Validate connectivity from 'on-premises' to Azure

Duration: 30 minutes

In this exercise, you will validate connectivity from your simulated on-premises environment to Azure.

Task 1: Create a virtual machine to validate connectivity

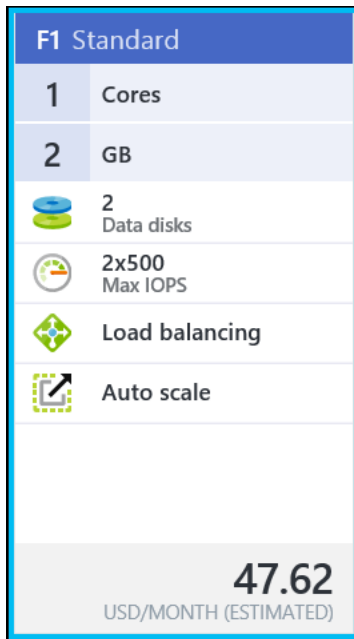
1. Create a new Virtual Machine in the second virtual network by clicking **New, Compute, and Windows Server 2016 Datacenter**.
2. Specify the following configuration, and click **OK**. See the following screenshot for more details.
 - Name: **OnPremVM**
 - User name: **demouser**
 - Password: **demo@pass123**
 - Resource Group: Create new: **OnPremVMRG**
 - Location: **the region you created the OnPremSimVNet virtual network in (East US)**.



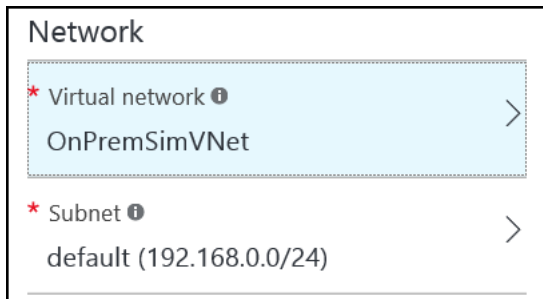
The screenshot shows the 'Basics' configuration window for a new Azure Virtual Machine. The window is titled 'Basics' and has a close button in the top right corner. The configuration fields are as follows:

- Name:** OnPremVM (with a green checkmark)
- VM disk type:** SSD (with a dropdown arrow)
- User name:** demouser (with a green checkmark)
- Password:** demo@pass123 (with a green checkmark and a password icon)
- Confirm password:** demo@pass123 (with a green checkmark and a password icon)
- Subscription:** (with a dropdown arrow)
- Resource group:** OnPremVMRG (with a green checkmark and radio buttons for 'Create new' and 'Use existing')
- Location:** East US (with a dropdown arrow)

3. On the **Size** blade, choose **F1 Standard**, and click **Select**.



- On the **Settings** blade, change the Virtual network to **OnPremSimVNet**, and set the subnet to the default subnet named: **default**.

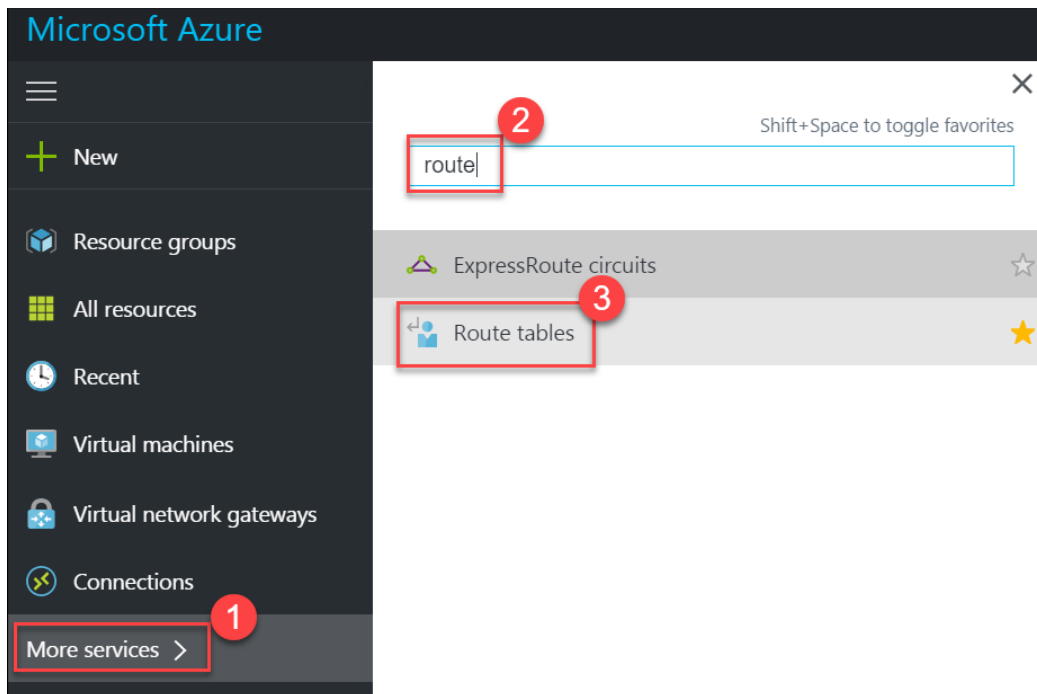


- Click **OK** twice to provision the virtual machine.

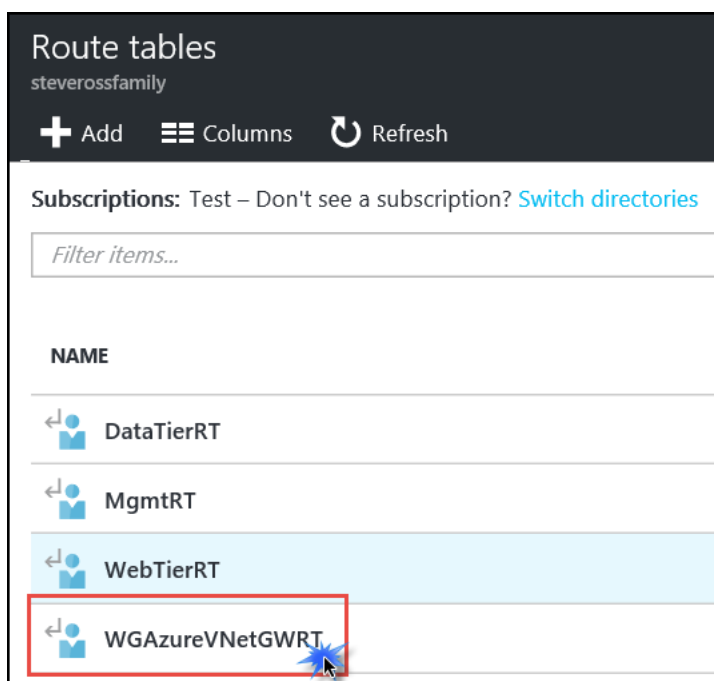
Task 2: Configure routing for simulated 'on-premises' to Azure traffic

When packets arrive from the simulated 'on-premises' virtual network (OnPremSimVNet) to the 'Azure-side' (WGVNET), they arrive at the gateway (WGAzureVNetGW). This gateway is in a gateway subnet (10.7.0.16/29). For packets to be directed to the pfSense firewall, we need another route table and route to be associated with the gateway subnet on the 'Azure' side.

- On the main portal menu to the left, click **More services** at the bottom. Enter **route** in the search box, and click on **Route tables**.



2. On the **Route tables** blade, click **Add**.
3. On the **Route table** blade, enter the following information:
 - a. Name: **WGAzureVNetGWRT**
 - b. Subscription: **Choose your subscription**
 - c. Resource group: Select **Use existing**, click the drop-down menu, and select **WGVNetRG**
 - d. Location: Same region where WGVnet exists
 - e. Click **Create**.
4. Click on **WGAzureVNetGWRT** route table.



5. Click **Routes**.
6. On the **Routes** blade, click the **+Add** button. Enter the following information, and then click **OK**:
 - a. Route name: **OnPremToWebTier**
 - b. Address prefix: **10.7.1.0/24**
 - c. Next hop type: **Virtual appliance**
 - d. Next hop address: **10.7.0.4**

Add route
WGAzureVNetGWRT

* Route name
OnPremToWebTier ✓

* Address prefix ⓘ
10.7.1.0/24 ✓

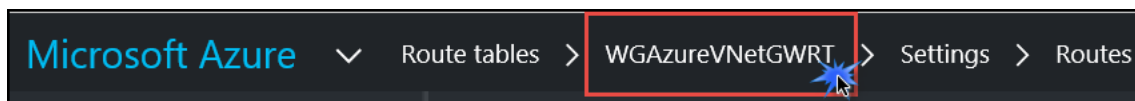
Next hop type ⓘ
Virtual appliance ▼

* Next hop address ⓘ
10.7.0.4 ✓

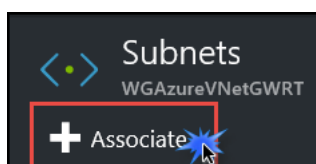
Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

OK

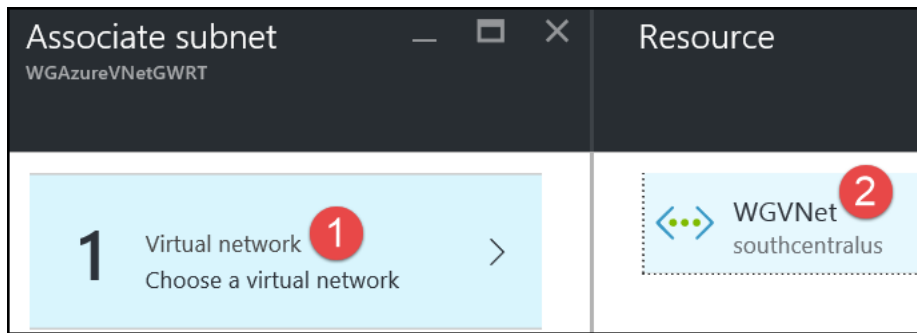
7. Using the breadcrumb menu at the top of the portal, navigate back to the **WGAzureVNetGWRT** route table settings.



8. On the **Settings** blade, click on **Subnets**.
9. On the **Subnets** blade click on the **Associate** link.



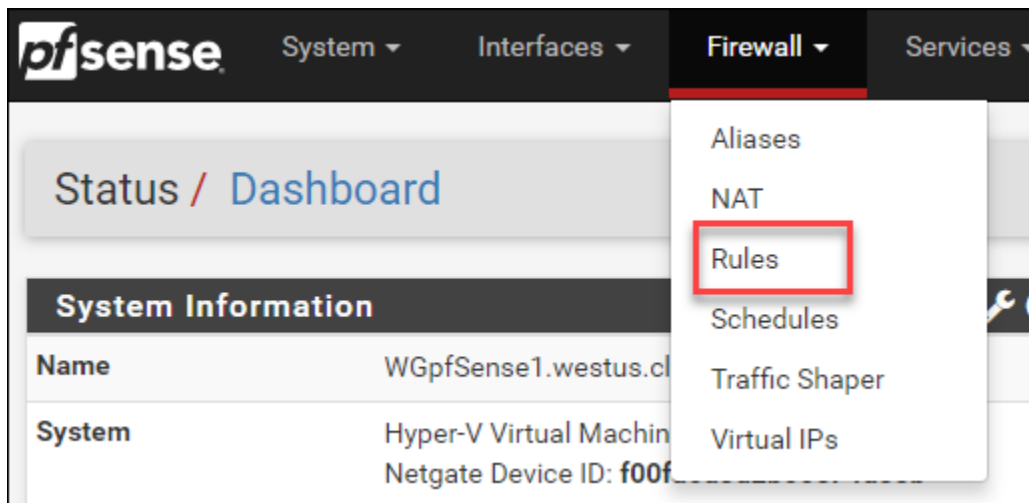
10. On the **Associate subnet** blade click on **Virtual Network**. Then click on **WGVNet**.



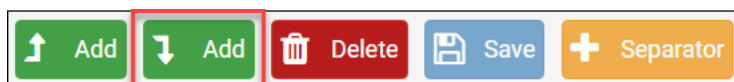
11. The **Choose subnet** blade opens. Click on **Gateway Subnet**. Then click **OK** at the bottom to complete the association.

Task 3: Add a firewall rule on pfSense

- In a browser on your local machine, navigate to the Public IP address of your pfSense firewall. If you followed the preceding instructions, it will be in this format: <https://<publicIPofpfSense:8443>
- Log on using:
 - User: **demouser**
 - Password: **demo@pass123**
- Hover over **Firewall** and click on **Rules**.



4. At the bottom of the list of rules, click the + icon to add a firewall rule



- Make the following changes to the default settings, see the following screenshot for more details:
 - Type: **Network**
 - Address: **192.168.0.0/24**

- b. Destination
 - i. Type: **Network**
 - ii. Address: **10.7.1.0/24**
- c. Destination port range:
 - i. From: Choose **HTTP (80)** from drop-down
- d. Description: **From OnPrem to Web Tier**

Click **Save**.

Firewall / Rules / Edit

Edit Firewall Rule

Action

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface

Choose the interface from which packets must come to match this rule.

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.

Source

Invert match. /

Display Advanced

Destination

Invert match. /

Destination port range

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

A description may be entered here for administrative reference.

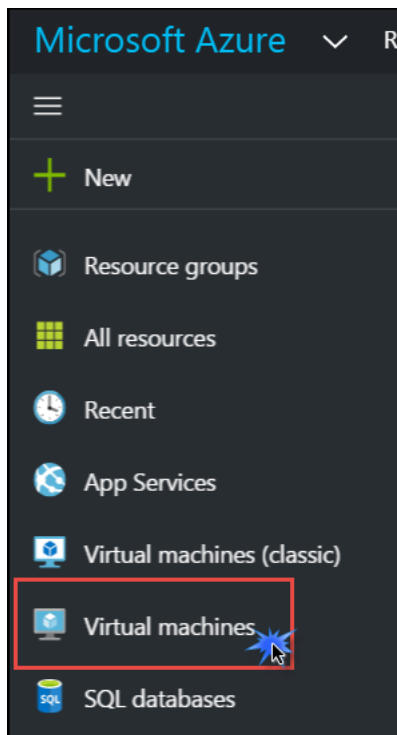
Advanced Options

6. Click **Apply changes**.

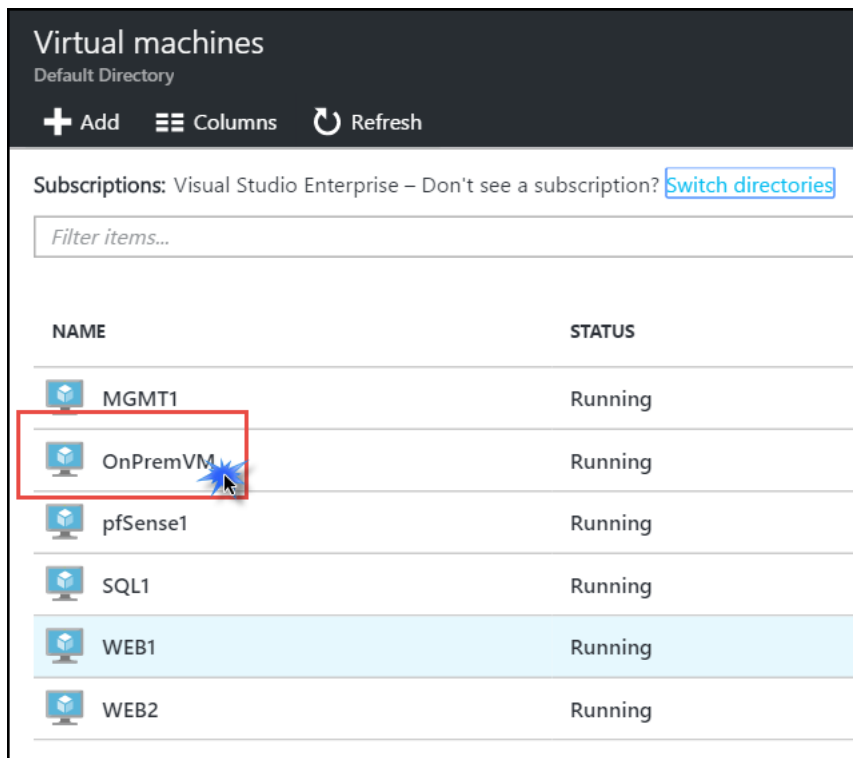
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Task 4: Validate connectivity from 'on-prem' to 'Azure' side

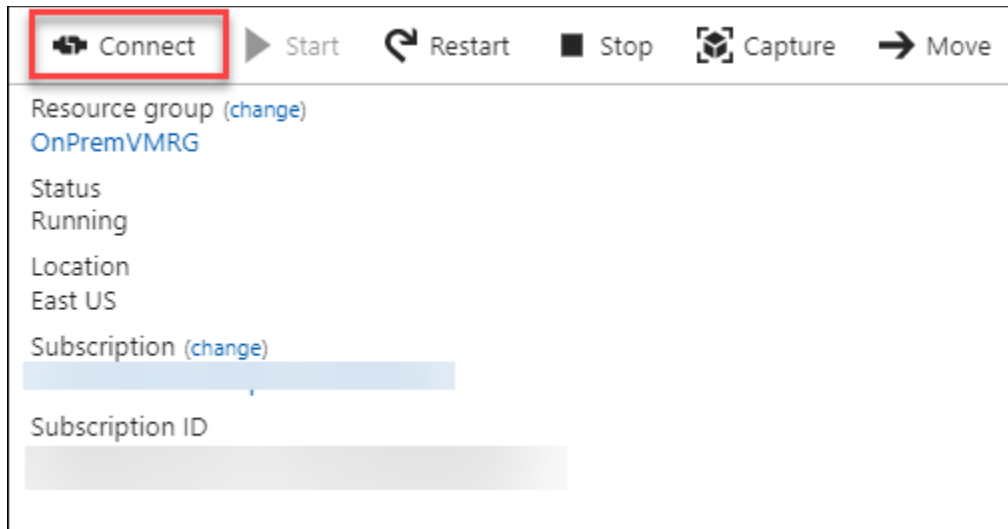
1. Click **Virtual machines** on the main Azure menu.



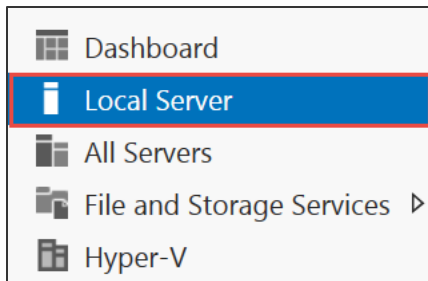
2. In the list of VMs, click **OnPremVM**.



3. On the **Essentials** blade, click **Connect** to open an RDP session to **OnPremVM**.



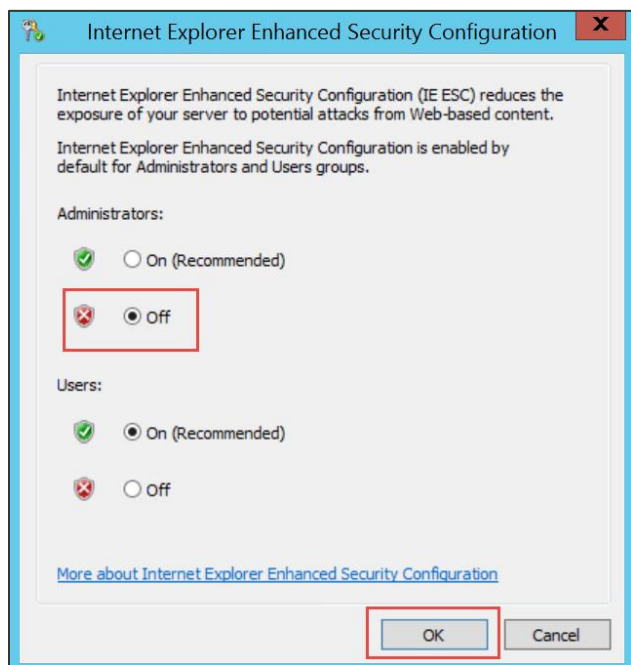
4. Log on with the following credentials:
 - a. Username: **demouser**
 - b. Password: **demo@pass123**
5. Once you have logged on, open **Server Manager** (if it is not already opened).
6. On the left, click **Local Server**.



7. On the right side of the pane, click **On** by **IE Enhanced Security Configuration**.

Last installed updates	Never
Windows Update	Install updates automatically using Windows Update
Last checked for updates	Never
Windows Error Reporting	Off
Customer Experience Improvement Program	Not participating
IE Enhanced Security Configuration	On
Time zone	(UTC) Coordinated Universal Time
Product ID	00253-50000-00000-AA006 (activated)
Processors	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz
Installed memory (RAM)	3.5 GB
Total disk space	177 GB

8. Change to **Off** for Administrators, and click **OK**.



9. Open Internet Explorer, and navigate to <http://10.7.1.10>. This should open the CloudShop app via the load balancer's internal IP. If you refresh the browser several times, you should see the server name changing:

CloudShop Demo - Products - running on WEB1

CloudShop Demo - Products - running on WEB2

After the hands-on lab

Duration: 10 minutes

After you have successfully completed the Enterprise-class networking in Azure hands-on lab step-by-step, you will want to delete the Resource Groups. This will free up your subscription from future charges.