Exercise: Configure Azure Firewall

Introduction

If you have been following along with the activities and exercises, the Sam's Scoops network should have the following components:

- A resource group **RG_Web_Server** with a VM called **SamScoopsWeb**.
- A **Firewall** resource group with a VNet called **Firewall-Hub** containing the **AzureFirewallSubnet**.

These VNets should also be peered to communicate with one another.

By now you know how the different Microsoft Azure firewall SKUs can be used to protect networks and devices within Microsoft Azure. In this exercise you will deploy and configure an Azure Standard Firewall to begin the process of protecting devices and networks within an Microsoft Azure environment.

Case study

With the VM for the Sam's Scoops webserver in place and the hub-spoke network topology set up, its time to install an Azure Standard Firewall to protect the network and its resources. You also need to provide remote access via the firewall as well as access to additional protocols so that a web developer can develop the web server.

Instructions

For this exercise to be successful the exercise *Create a Windows virtual machine in the Azure portal* from Lesson 2 has to have been completed and the machine still needs to be present. If not, please revisit that exercise first.

Step 1: Firewall deployment

Traffic on the Sam' Scoops network will fluctuate since demand for its products will most likely increase over weekends, holidays and hot weather. That's why an Azure Standard Firewall is the best fit for the business. To deploy the Azure Standard Firewall on the **Firewall-Hub 192.168.1.0** subnet follow these steps:

1. Sign into your Azure subscription from the Azure portal.
2. On the Azure home page, select **Firewalls** under the Azure services bar.
3. Select on **Create Firewall**.
4. Subscription: Select your subscription.

5. Resource group: Select the **Firewall** resource group from the dropdown, created in the earlier activity.
6. Give the firewall instance the name "ScoopsFirewall".
7. Region: Select the same location that you have used previously.
8. Firewall SKU: Select **Standard** from the Firewall SKU selection boxes.
9. For firewall management, select **Use Firewall rules (classic) to manage this firewall**.
10. For **Choose a virtual network** select **Use existing** and select the **Firewall-Hub** network for the virtual network created in a previous activity.
11. IP address: For the **Public IP address** select **Add new** and give it the name "FirewallScoops", select **OK**.
12. Select **Review + create.** The firewall will now be deployed.

Step 2: Firewall application rule creation

The web server will need access to Google once it is set up, so an application rule needs to be setup to allow outbound access. To do this, follow these steps:

1. Open the **Firewall** resource group, and select the **ScoopsFirewall** firewall.
2. On the **ScoopsFirewall** page, under **Settings**, select **Rules (classic)**.
3. Select the **Application rule collection** tab.
4. Select **Add application rule collection**.
5. For **Name**, type "AppRule1".
6. For **Priority**, type " 200".
7. For **Action**, select **Allow**.
8. Under **Rules**, **Target FQDNs**, for **Name**, type "Allow-Google".
9. For **Source** type, select **IP address**.
10. Type **172.16.1.0/24** for the **Source.**
11. For **Protocol:port**, type "http, https".
12. For **Target FQDNS**, type "www.google.com".
13. Select **Add** and after a while the rule will be created.

Step 3: Firewall network rule creation

The web server will also need to use DNS to resolve IP addresses so you need to create a network rule to allow this. Follow these steps to do this:

1. Select the **Network rule collection** tab.
2. Select **Add network rule collection**.
3. For **Name**, type "Net-Rule1".
4. For **Priority**, type "200".
5. For **Action**, select **Allow**.
6. Under **Rules**, **IP addresses**, for **Name**, type "Allow-DNS".
7. For **Protocol**, select **UDP**.
8. For **Source type**, select **IP address**.
9. Type **172.16.1.0/24** for the **Source**.
10. For **Destination type** select **IP address**.
11. For **Destination address**, type **209.244.0.3,209.244.0.4** (These are public DNS servers operated by Level 3)
12. For **Destination Ports**, type "53".
13. Select **Add**.

Step 4: Firewall NAT rules creation

To allow the web developer to setup the web server you need to provide remote access to the VM. Follow these steps to create a destination NAT rule for RDP.

1. Select the **NAT rule collection** tab.
2. Select **Add NAT rule collection**.
3. For **Name**, type " rdp".
4. For **Priority**, type "200".
5. Under **Rules**, for **Name**, type "rdp-nat".
6. For **Protocol**, select **TCP**.
7. For **Source type**, select **IP address**.

8. Type "*.(* = anything)" for the **Source**.
9. For **Destination address**, type the firewall public IP address.
10. For **Destination Ports**, type "3389".
11. For **Translated address**, type the **SamScoopsWeb** virtual machine's private IP address.
12. For **Translated port**, type "3389".
13. Select **Add**.

Step 5: Advanced threat protection

Earlier you learned that one of the great advantages of using the Azure Standard Firewall is the automatic rule creation for threats with Threat Intelligence. But recall that by default, the firewall is set to only create threat alerts. Follow these steps to enable the alert and deny option.

1. On the **ScoopsFirewall** page, under **Settings**, select **Threat Intelligence**.
2. For **Threat Intel mode** select **Alert and deny**.
3. Select **Save**.

Clean-up

Note: Once you have finished with this exercise please delete the Standard Firewall as it cannot be powered off and you will continue being charged if it stays active.

If you are using your own Azure subscription, it is recommended that you follow the clean-up instructions to stop compute resources after completing each lesson. When you're working in your own subscription, it's also a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

Please refer to the reading, *Clean up resources* for instructions on how to delete resources after you've completed the exercise.

Conclusion

You have now configured and deployed an Azure Standard Firewall that will protect the Sam's Scoops virtual machine and network. By enabling remote access, you made it possible for a web developer to develop a web server on this virtual machine. The virtual machine is also protected by a centrally installed firewall that only allows DNS traffic and access to the Google web page for the virtual machine.