Networking Lab 12

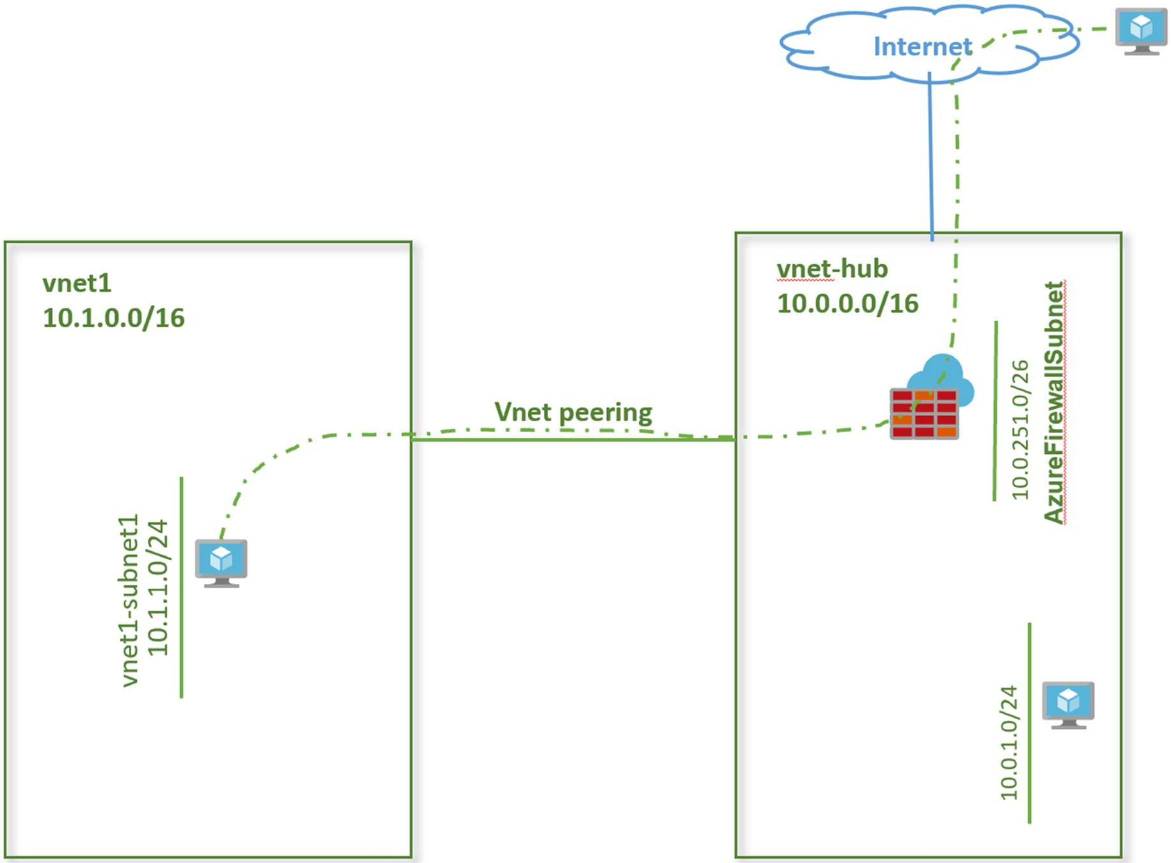
Azure Firewall

Author:
Binal Shah
Principal Cloud Solution Architect, Microsoft

Lab Overview

In this lab, we will deploy the Azure firewall and explore the firewall features. Azure firewall provides ability to have a centralized control on firewall rules for traffic going out and in of virtual networks. Azure firewall also provides FQDN filtering for outbound flows. In this lab, we will explore a hub-and-spoke topology, deploy the Azure firewall in the hub and add application rules to restrict traffic.

Lab Diagram



Create a firewall

We will deploy an Azure firewall in the virtual network vnet-hub. Azure firewall requires a dedicated subnet with the name AzureFirewallSubnet. We will first create the dedicated subnet and then deploy the firewall.

Create a firewall subnet in the hub virtual network

1. Go to the search bar at the top of the page and type *virtual network*. Select **Virtual Networks** from the dropdown list.
2. From the list of vnets, click on **vnet-hub**.
3. Under **Settings**, click on **Subnets**. Then click **+Subnet** to add a new firewall subnet.
4. Add the following values, leave the other default settings, and then select **Create**.

Name	Enter *AzureFirewallSubnet*
Address range	Enter *10.0.251.0/24*

Deploy Azure firewall in the hub virtual network

1. From the portal home page, select **Create a resource**.
2. Type **firewall** in the search box and press **Enter**.
3. Select Azure **Firewalls** and then select **Create**.
4. On the **Create a Firewall** page, use the following table to configure the firewall:

Setting	**Value**
Subscription	<your subscription>
Resource group	**rg-lab**
Name	**vnet-hub-fw**
Region	**West US 2**
Choose a virtual network	**Use existing** and select **vnet-hub** from the dropdown
Public IP address	**Create new**. The Public IP address must be the Standard SKU type. Give a name to the new Public IP resource as **vnet-hub-fw-ip1**

5. Select **Review + create**.
6. Review the summary, and then select **Create** to create the firewall.
   This will take a few minutes to deploy.
7. After deployment completes, go to the **rg-lab** resource group, and select the **vnet-hub-fw** firewall.
8. Note the private IP address. You'll use it later when you create the default route.

Configure an application rule

This is the application rule that allows outbound access to www.microsoft.com

1. Go to the resource group **rg-lab**, and select the firewall **vnet-hub-fw** firewall.
2. On the **vnet-hub-fw** firewall page, under **Settings**, select **Rules**.
3. Select the **Application rule collection** tab.
4. Select **Add application rule collection**.
5. For **Name**, type **application-rule1**.
6. For **Priority**, type **200**.
7. For **Action**, select **Allow**.
8. Under **Rules**, **Target FQDNs**, for **Name**, type **allow-Microsoft**.
9. For **Source Addresses**, type **10.1.1.0/24**.
10. For **Protocol:port**, type **http, https**.
11. For **Target FQDN**, type **www.microsoft.com**
12. Select **Add**.

Create a custom route in the spoke vnet

Create a route table in region West US 2.

1. From the Azure portal home page, select **Create a resource**.
2. In the search text box, type **route table** and press **Enter**.
3. Select **Route table**.
4. Select **Create**.
5. For the name, type **udr-to-fw**.
6. Select **rg-lab** for the resource group.
7. For **Location**, select location West US 2.
8. Select **Create**.

Add custom route in the route table.

1. After the route table is created, select it to open the route table page.
2. Select **Routes** in the left column.
3. Select **Add**.
4. For the route name, type **default-to-fw**.
5. For the address prefix, type **0.0.0.0/0**.
6. For next hop type, select **Virtual appliance**.
7. For next hop address, type the firewall's private IP address that you noted earlier.
8. Select **OK**.

Now associate the route to the subnet.

1. On the **udr-to-fw Route table** page, select **Subnets**.
2. Select **Associate**.
3. Select **Choose a virtual network**.

4. Select **vnet1**.
5. Select **vnet1-subnet1**.
6. Select **OK**.

Test the firewall

Now, test the firewall to confirm that it works as expected.

1. From the Azure portal, go to the virtual machines page and click on virtual machine **vnet1-vm-mgmt1.** If you don't have a virtual machine in vnet1, run the following commands in cloud shell to deploy a new virtual machine:

   ```
   ResourceGroup=rg-lab
   VmName=vnet1-vm-mgmt1
   SubnetName=vnet1-subnet1
   VnetName=vnet1
   AdminUser=azureuser
   AdminPassword=Azure123456!
   az vm create --resource-group $ResourceGroup --name $VmName --image UbuntuLTS --vnet-name $VnetName --subnet $SubnetName --admin-username $AdminUser --admin-password $AdminPassword --nsg "" --asg mgmt
   ```

2. Under Support + troubleshooting, click on **Serial console**. Login with username and password.
3. From the shell, run the following command to reach the Microsoft website:
   wget www.microsoft.com
   The page contents loaded successfully.
4. Now, run the same command to reach www.youtube.com
   wget www.youtube.com
   You should receive an error message. This site is successfully blocked by the firewall.
   HTTP request from 10.1.1.4:54192 to www.youtube.com:80. Action: Deny. No rule matched. Proceeding with default action

Conclusion

We have reviewed how to configure the Azure firewall. We verified the firewall can be used in a hub and spoke topology to centralize firewall rules. We also saw how Azure firewall supports FQDN filtering for outbound traffic.