How to Configure Azure Route Tables (UDR) using Azure Portal and ARM

https://campus.barracuda.com/doc/47579402/

Azure Route Tables, or User Defined Routing, allow you to create network routes so that your F-Series Firewall VM can handle the traffic both between your subnets and to the Internet. For the network interfaces to be allowed to receive and forward traffic, IP forwarding must be enabled. When different route types are present in a UDR route table, user defined routes are preferred over the default system routes. When multiple routes match the destination, the more specific route is used. The default system routes always present in an Azure route table allow the following:

- Traffic within the virtual network
- Traffic to the Internet
- Traffic between different virtual networks using Azure VPN Gateway
- Traffic from the virtual network to networks connected via Azure VPN Gateway

In this article:

Limitations

- Multiple network interfaces are not supported for high availability clusters.
- Multiple network interfaces in one subnet are not supported for stand-alone firewall VMs.

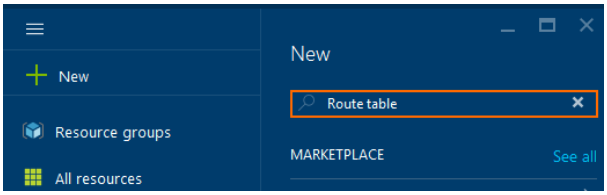
Before vou begin

- Deploy a Barracuda NextGen Firewall F. For more information, see Microsoft Azure Deployment.
- To enable IP forwarding: Install Azure PowerShell 1.1.0 or higher.

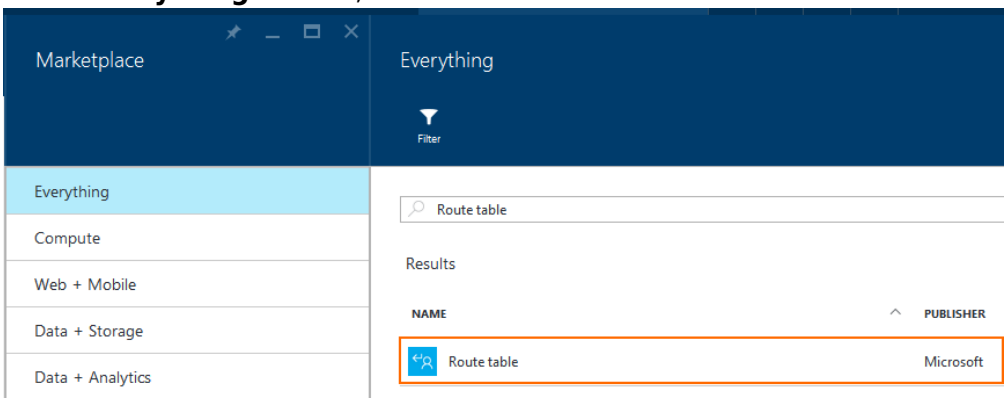
Step 1. Create an Azure Route Table

Create a route table in the networking resource group.

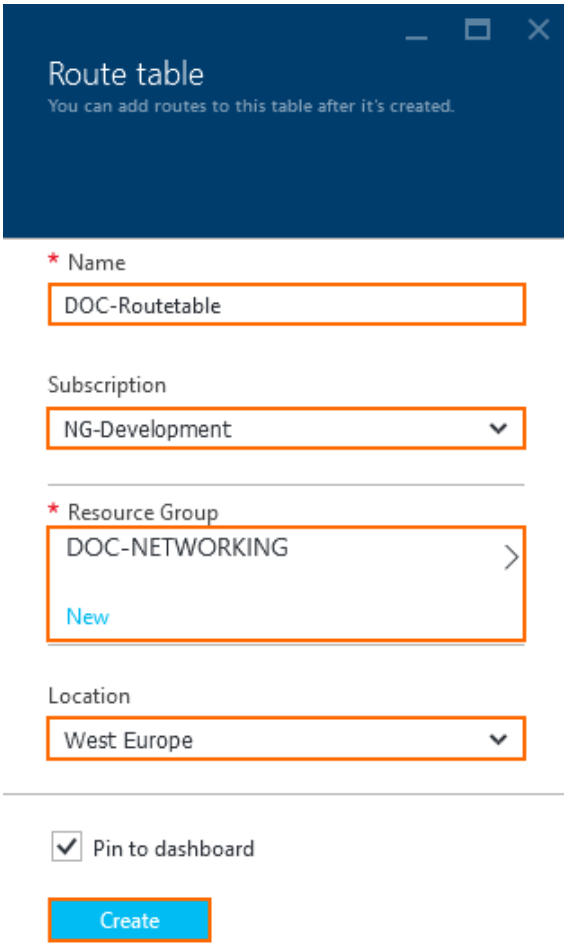
1. Log into the Azure Portal: https://portal.azure.com.
2. Click **New**.
3. In the **New** column, select **Route table** in the search box and press **Enter**.



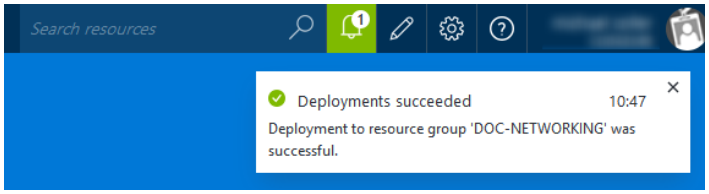
4. In the **Everything** column, select **Route table**.



5. Click **Create**.
6. In the **Route table** column, enter:
   - **Name** – Enter the route table name.
   - **Subscription** – Select the Azure subscription.
   - **Resource Group** – Click **Select existing** to use an already existing resource group, or enter a unique resource group name to create a new resource group.
   - **Location** – Select the Azure datacenter where you want to deploy your VM. The route table must be in the same location as the virtual network and the VMs.
7. Click **Create**.



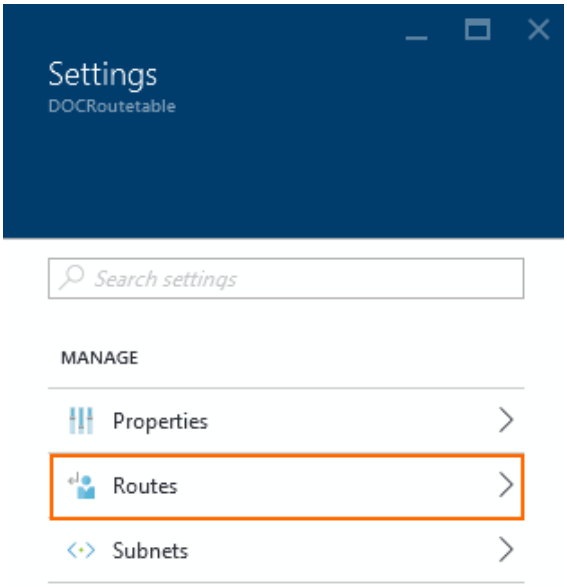
Wait for the route table deployment to finish.



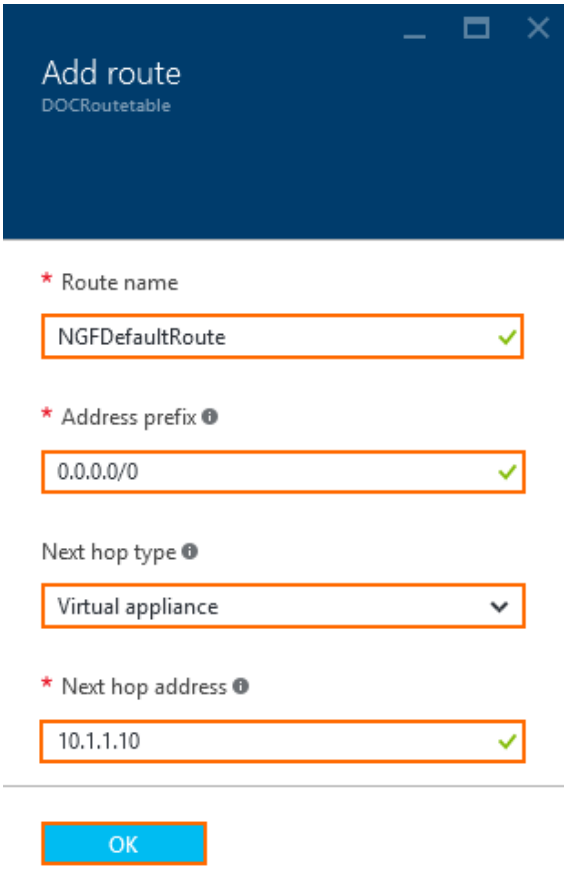
Step 2. Add routes

Create user defined routes to use your firewall VM as a gateway.

1. Log into the Azure Portal: https://portal.azure.com.
2. Open the route table created in step 1.
3. In the **Settings** column, click **Routes**.

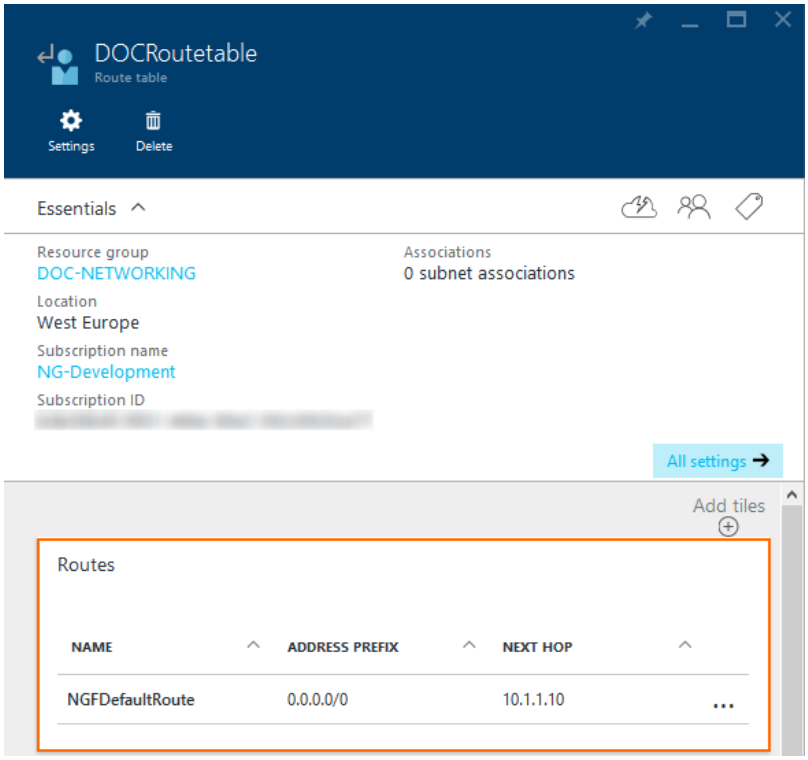


4. In the **Routes** column, click **+ Add**.
5. In the **Add route** column, enter:
   - **Route name** – Enter a unique route name.
   - **Address prefix** – Enter the destination IP address range in CIDR. Use `0.0.0.0/0` to create a default route.
   - **Next hop type** – Select **Virtual appliance**.
   - **Next hop address** – Enter the private IP address of the F-Series Firewall VM. If you are using an HA cluster, enter the IP address of the active firewall VM.



6. Click **OK**.
7. (optional) Create additional routes.

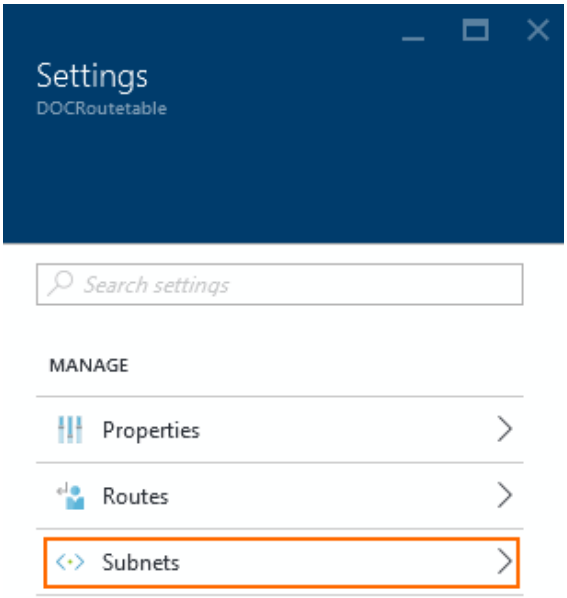
The routes you created are now visible in your route tables column.



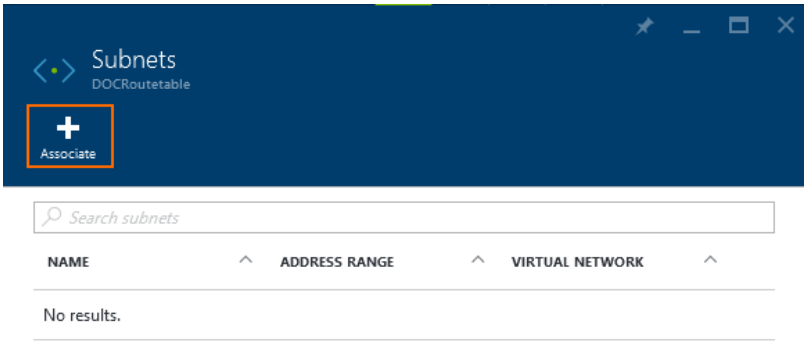
Step 3. Associate the route table with the subnets

Assign the routing table to the subnets. It is not possible to associate more than one routing table with a subnet.

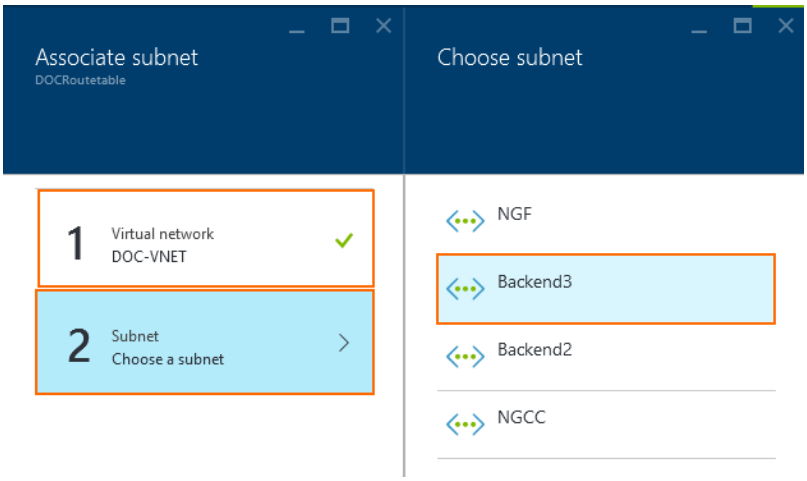
1. Log into the Azure Portal: https://portal.azure.com.
2. Open the route table created in step 1.
3. In the **Settings** column, click **Subnets** .



4. In the **Subnets** column, click **Associate** to add a subnet.



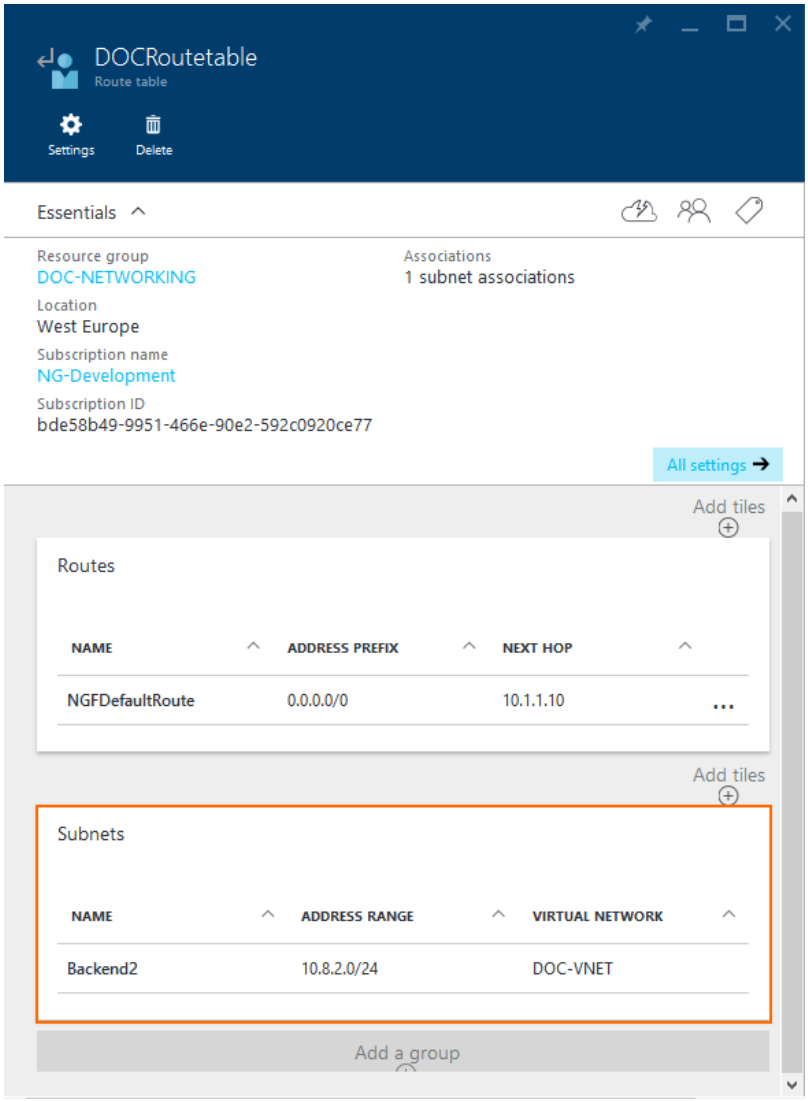
5. In the **Associate subnet** column, click **Virtual network**.
6. Select the virtual network in the **Resource** column
7. In the **Associate subnet** column, click **Subnet.**
8. In the **Choose subnet** column, select the subnet.



9. Click **OK**.
10. (optional) Associate additional subnets with the route table.

The subnets associated with this route table are now visible in the subnets section of your route

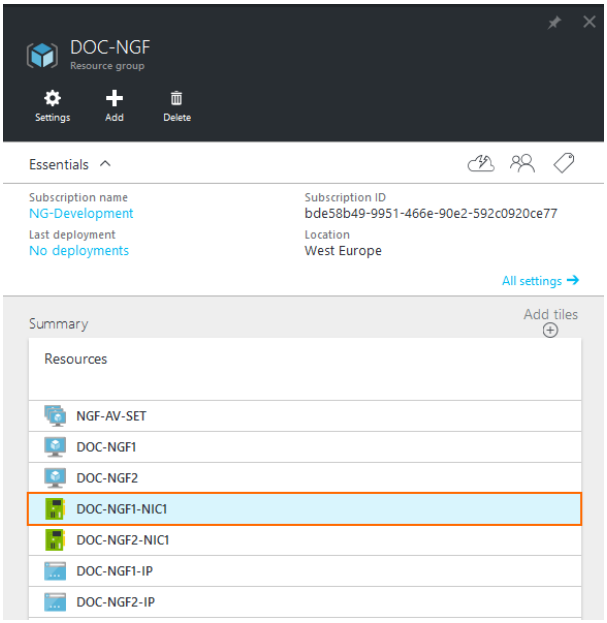
tables column:



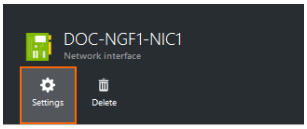
Step 4. Enable IP forwarding for the network interfaces of the firewall VM

Enable IP forwarding for all attached network interfaces of the firewall VM. This enables the firewall to forward traffic with a destination IP address that does not match its own private IP address.

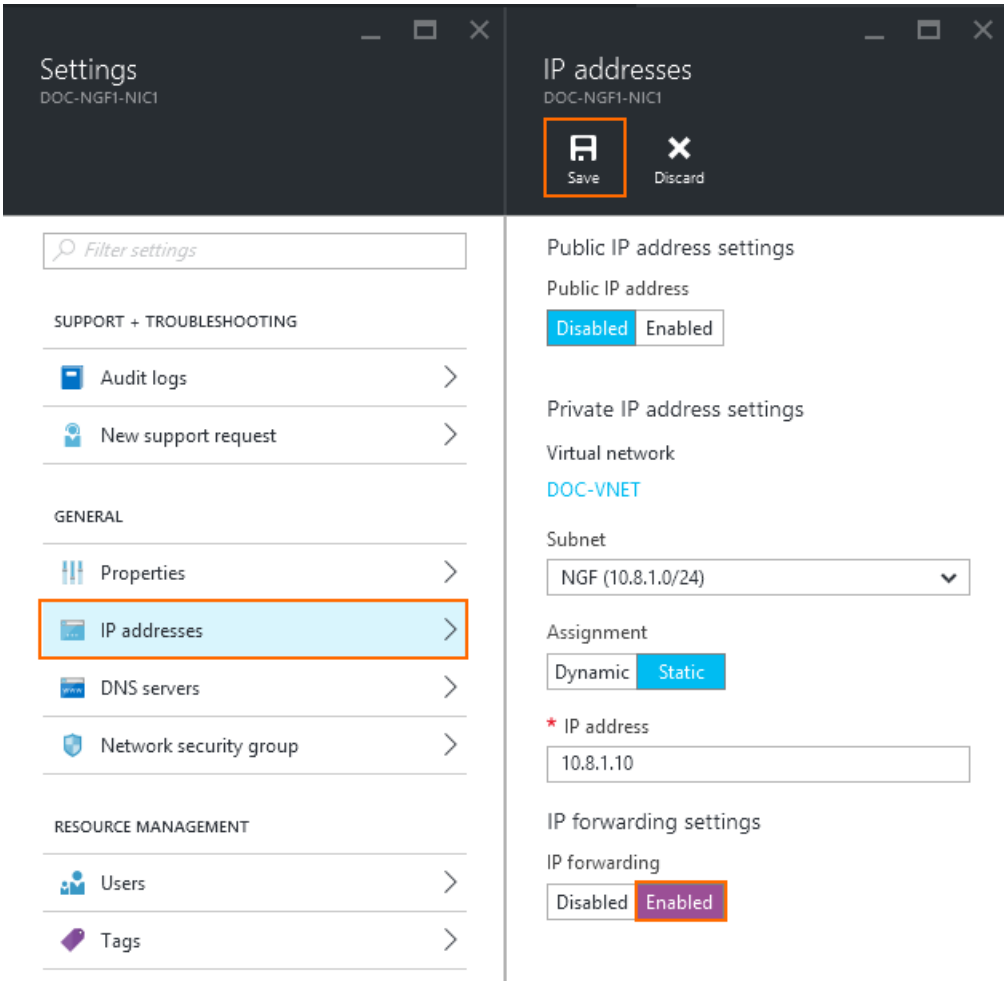
1. Log into the Azure Portal: https://portal.azure.com.
2. Open the network interface attached to your firewall VM.



3. In the **Network Interface** column, click **Settings**.



4. In the **Settings** column, click **IP addresses**.
5. In the **IP addresses** column, set **IP forwarding** to **Enabled**.
6. Click **Save**.



The Barracuda NextGen Firewall F VM can now forward traffic from backend VMs to the Internet.

Next Steps

- Create access rules to allow traffic from the backend VMs to the Internet. For more information, see Firewall Access Rules.
- Configure UDR route rewriting to display the Azure route table in NextGen Admin. For more information, see How to Configure Azure Route Table Rewriting for HA Clusters using ARM.

Figures

1. udr_portal_01.png
2. udr_portal_02.png
3. udr_portal_03.png
4. udr_portal_04.png
5. udr_portal_05.png
6. udr_portal_06.png
7. udr_portal_07.png
8. udr_portal_08.png
9. udr_portal_09.png
10. udr_portal_10.png
11. udr_portal_11.png
12. ip_forwarding_01.png
13. ip_forwarding_02.png
14. ip_forwarding_03.png