How to Configure Azure Route Tables (UDR) in Azure using PowerShell and ASM

https://campus.barracuda.com/doc/48202628/

Azure allows you to change the routing in your VNET with Azure User Defined Routes (UDR). You must enable IP forwarding for the Barracuda NextGen Firewall F-Series and then create and configure the routing table for the backend networks, so all traffic is routed through the Barracuda NextGen Firewall F-Series in the frontend subnet. The Azure routing table can be assigned to multiple backend subnets. F-Series Firewalls using multiple network interfaces do not support high availability deployments.

Limitations

After the Azure routing table has been applied, the VMs in the backend networks are only reachable via the NextGen Firewall F-Series. This also means that existing Endpoints allowing direct access no longer work.

Before you begin

- Deploy a Barracuda NextGen Firewall F-Series in the Azure cloud. For more information, see Microsoft Azure Deployments using Azure Service Manager (ASM).
- Install Azure PowerShell version 0.9.8 or higher.

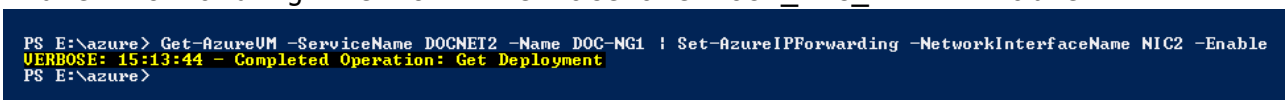
Step 1. Enable IP forwarding for the Barracuda NextGen Firewall F-Series VM

To forward traffic, you must enable IP forwarding for each network interface on the Barracuda NextGen Firewall F-Series VM.

1. Open Azure PowerShell.
2. To enable **IP forwarding** for the primary network interface, enter:
   `Get-AzureVM -ServiceName YOUR_CLOUD_SERVICE -Name YOUR_VM_NAME | Set-AzureIPForwarding -Enable`

   ```
   PS E:\azure> Get-AzureVM -ServiceName DOCNET2 -Name DOC-NG2 | Get-AzureIPForwarding
   VERBOSE: 13:49:51 - Completed Operation: Get Deployment
   Enabled
   PS E:\azure>
   ```
3. If you are using a Barracuda NextGen Firewall F-Series VM with more than one network interface, you must also enable **IP forwarding** on the other network interfaces:
   `Get-AzureVM -ServiceName YOUR_CLOUD_SERVICE -Name YOUR_VM_NAME | Set-`

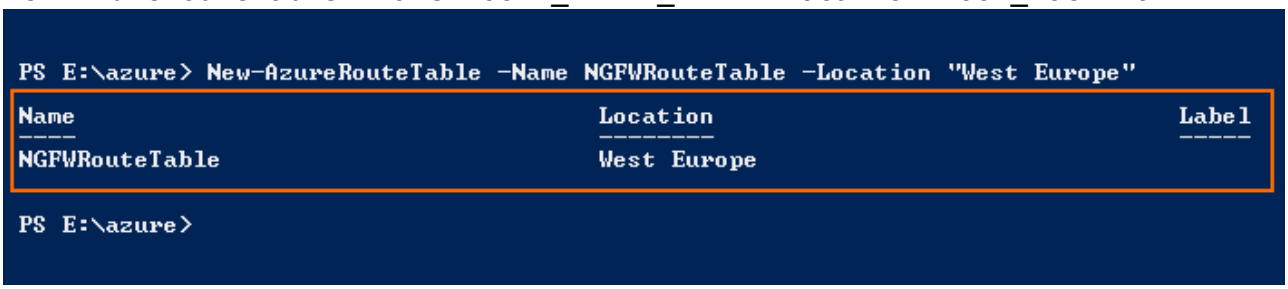
```
AzureIPForwarding -NetworkInterfaceName YOUR_NIC_NAME -Enable
```

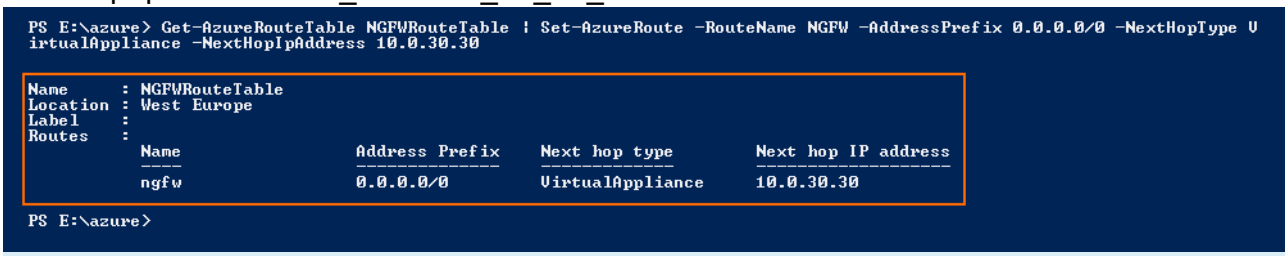


On the Azure networking level, your Barracuda NextGen Firewall F-Series VM is now allowed to forward IP packets. See the troubleshooting section below on how to check if IP forwarding is enabled for your interfaces.

Step 2. Create an Azure route table

Create a routing table in Azure and apply it the backend subnets of the VNET. Add a user-defined route to the routing table to change the default route for all VMs in the backend subnets to the Barracuda NextGen Firewall F-Series VM. The routing table can be applied to multiple backend subnets.

1. Open Azure PowerShell.
2. Create a new **Azure Routing Table**:
   ```
   New-AzureRouteTable -Name ROUTE_TABLE_NAME -Location YOUR_LOCATION
   ```
   

3. Add the default route to the Azure Routing Table:
   ```
   Get-AzureRouteTable -Name YOUR_ROUTE_TABLE | Set-AzureRoute -RouteName
   ROUTE_NAME -AddressPrefix 0.0.0.0/0 -NextHopType VirtualAppliance -
   NextHopIpAddress IP_ADDRESS_OF_NG_FIREWALL
   ```
   

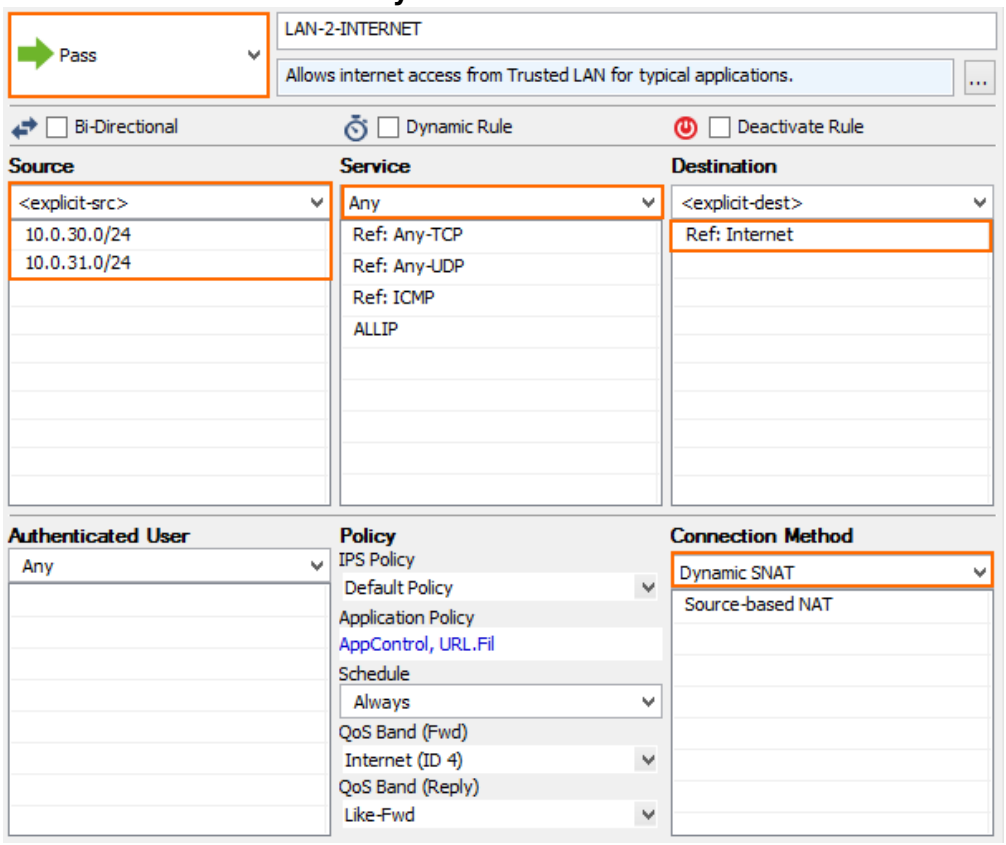
   The NextHopIPAddress for the default route is the IP address of a network interface of the Barracuda NextGen Firewall F-Series. It does not have to be in the same subnet, so NextGen Firewall F-Series VMs with just one network interface can be used for routing.
4. Assign the **Azure routing table** to the backend network:
   ```
   Set-AzureSubnetRouteTable -VirtualNetworkName YOUR_VNET_NAME -SubnetName
   SUBNET_NAME -RouteTableName YOUR_BACKEND_ROUTING_TABLE_NAME
   ```

All traffic from the backend subnets is now routed through the Barracuda NextGen Firewall F-Series VM. Propagating the routing table changes to the VMs in the subnets can take a couple of minutes. See the Troubleshooting section below on how to query Azure for the actual (effective) routing table used by the VM.

Step 3. Create access rules on the Barracuda NextGen Firewall F-Series

By default, all outgoing traffic from the backend is blocked by the NextGen Firewall F-Series. Create an access rule to allow access to the Internet.

1. Log into the Barracuda NextGen Firewall F-Series.
2. Create a **PASS** access rule:
   - **Source** – Enter the backend subnet networks.
   - **Service** – Select **Any**.
   - **Destination** – Select **Internet**.
   - **Connection** – Select **Dynamic SNAT**.



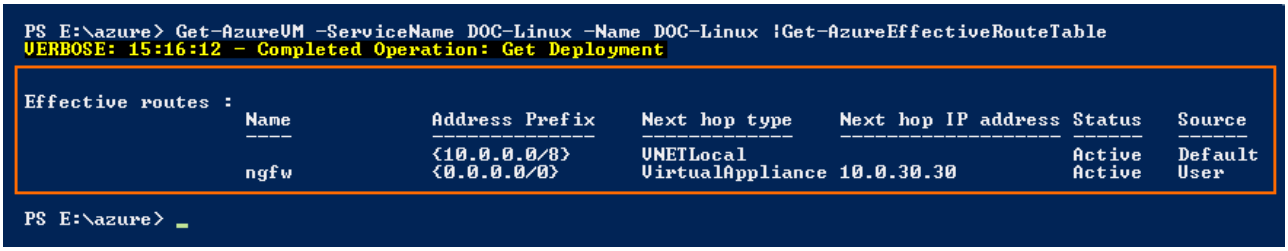
3. Click **OK**.
4. Place the access rule so that no access rule above it matches the same traffic.
5. Click **Send Changes** and **Activate**.

Your VMs in the backend networks can now access the Internet via the Barracuda NextGen Firewall F-

Series.

Troubleshooting

- Verify that IP forwarding is enabled for both network interfaces on the Barracuda NextGen Firewall F-Series.
  `Get-AzureVM -ServiceName CLOUD_SERVICE_NAME -Name VM_NAME | Get-AzureIPForwarding Get-AzureVM -ServiceName CLOUD_SERVICE_NAME -Name VM_NAME | Get-AzureIPForwarding -NetworkInterfaceName NIC2`
- Check the effective routing table used by the VMs in the backend networks.
  `Get-AzureVM -ServiceName DOCNET2 -Name DOC-NG2 | Get-AzureEffectiveRouteTable`



- If traffic is not forwarded through the NextGen Firewall F-Series even though it is enabled for each network interface and the correct access rule matches, try creating a new VNET. Using a new VNET requires you to redeploy your Barracuda NextGen Firewall F-Series VM.

Monitoring

Check **Network > Azure UDR** to see the UDR route table for the VNET. UDR routes pointing to the F-Series Firewalls are marked with a green icon.

Figures

1. UDR_01.png
2. UDR_01a.png
3. UDR_02.png
4. UDR_03.png
5. UDR_05.png
6. UDR_04.png