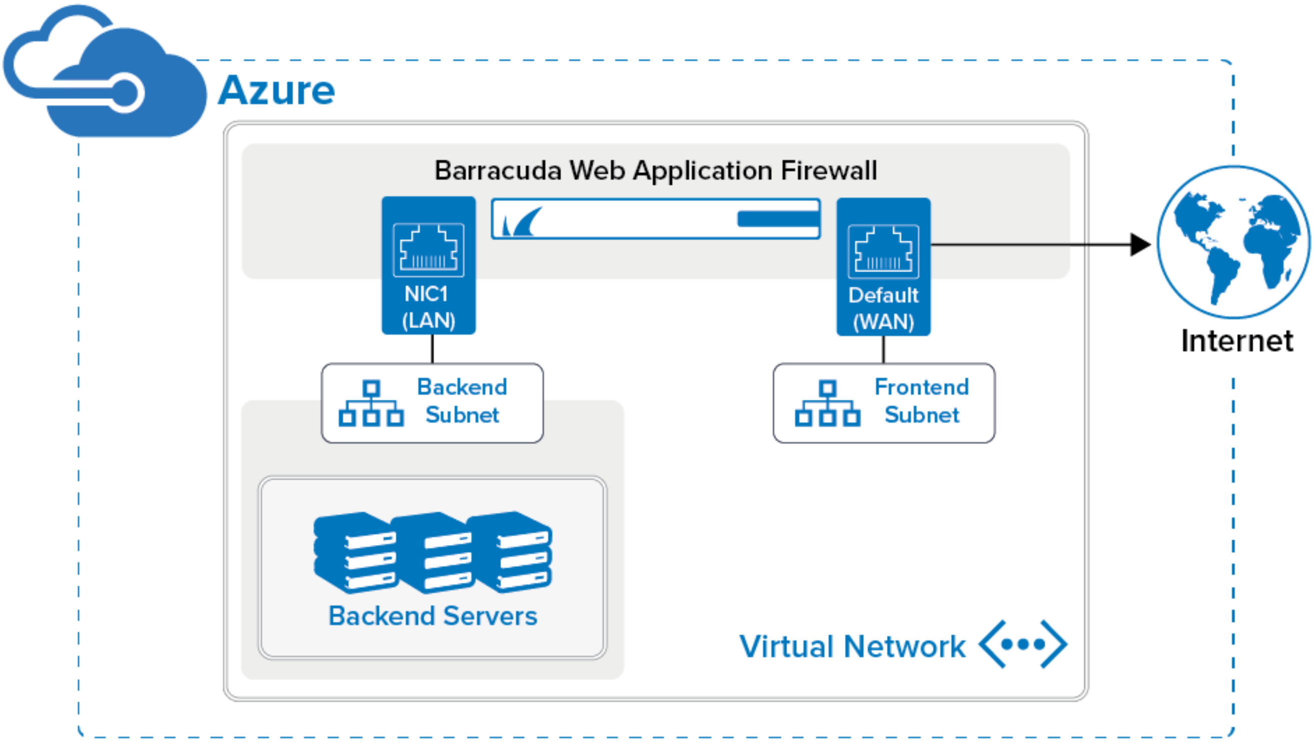
Configuring the Barracuda Web Application Firewall with Multiple NICs

https://campus.barracuda.com/doc/73007328/

You can deploy the Barracuda Web Application Firewall instances in Microsoft Azure and attach multiple network interface controllers (NICs) to it. Multiple NIC is a requirement for network appliances and virtual machines that forward the traffic from one subnet to another. Multiple NICs also provide more network traffic management functionality, including isolation of traffic between a front-end NIC and a backend NIC. Using Multiple NICs you can separate the data (WAN) traffic from the backend server (LAN) traffic, i.e., the servers can reside in the LAN network. For more information, refer to the Create a VM with multiple NICs article in the Microsoft Azure documentation.

You can deploy the Barracuda Web Application Firewall instance(s) with **Single NIC and Multi IP** or **Multi NIC and Multi IP** on Microsoft Azure using the Azure Resource Manager (ARM) template. See Configuring Multiple IP Addresses for the Barracuda Web Application Firewall Instance in Azure Resource Manager.

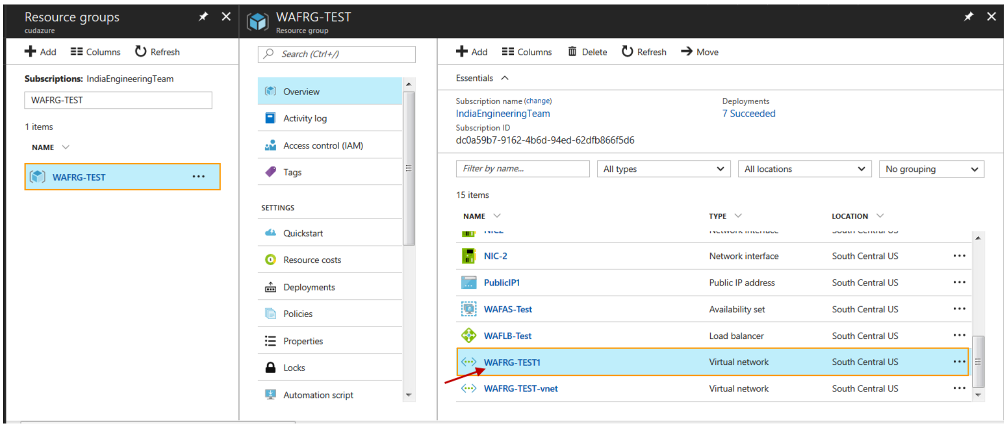


This article provides information on how to deploy the Barracuda Web Application Firewall instance with multiple NICs using Azure Resource Manager (ARM).

Prerequisite

To configure the Barracuda Web Application Firewall with multiple NICs, the virtual network should include two subnets, i.e., one for the WAN traffic and the other for the LAN traffic. When the Barracuda Web Application Firewall instance is deployed in Microsoft Azure, the virtual network is associated with a single subnet (i.e., for WAN traffic). To add another subnet, perform the following steps:

1. Log into the **Microsoft Azure** portal, click **Resource groups** on the left panel.
2. In the **Resource groups** list, click on the resource group to which the Barracuda Web Application Firewall instance is associated.
3. On the resource group page, click on the virtual network associated with the resource group.



Subscriptions: IndiaEngineeringTeam

WAFRG-TEST

1 items

NAME
WAFRG-TEST

Subscription name (change): IndiaEngineeringTeam

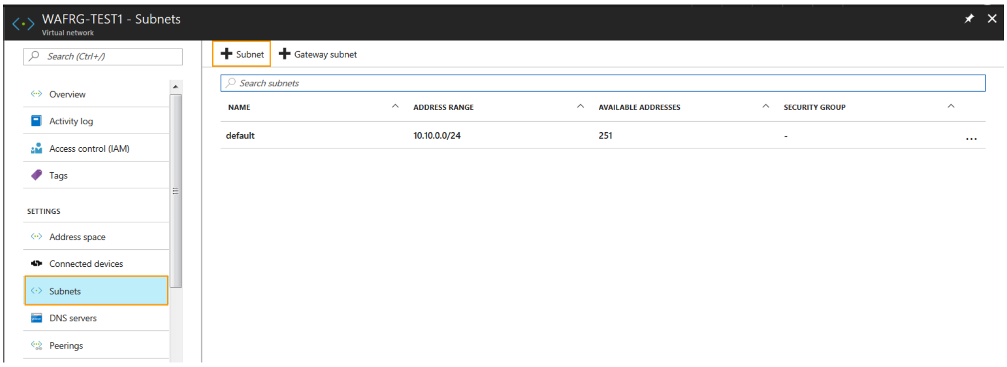
Deployments: 7 Succeeded

Subscription ID: dc0a59b7-9162-4b6d-94ed-62dfb866f5d6

15 items

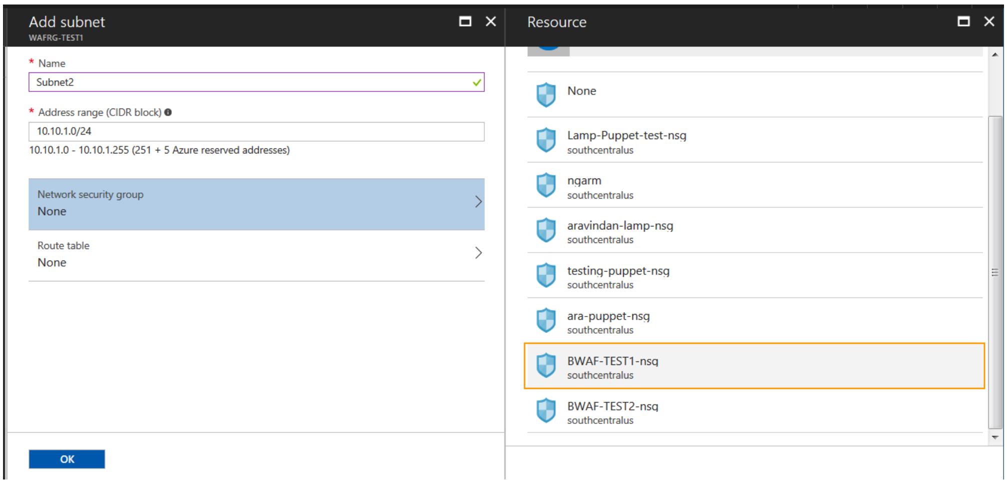
NAME	TYPE	LOCATION
NIC-2	Network interface	South Central US
PublicIP1	Public IP address	South Central US
WAFAS-Test	Availability set	South Central US
WAFLB-Test	Load balancer	South Central US
WAFRG-TEST1	Virtual network	South Central US
WAFRG-TEST-vnet	Virtual network	South Central US

4. On the virtual network page, select **Subnets** under **SETTINGS** and click **Subnet**.



NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
default	10.10.0.0/24	251	-

5. On the **Add Subnet** page:
    1. **Name**: Enter a name for the subnet.
    2. **Address range (CIDR block)**: Enter the IP address for the subnet. The IP address should be within the address space of the virtual network.
    3. **Network security group**: Select the network security group associated with the resource group selected in Step 2.
    4. Click **OK**.



* Name: Subnet2

* Address range (CIDR block): 10.10.1.0/24

10.10.1.0 - 10.10.1.255 (251 + 5 Azure reserved addresses)

Network security group: None

Route table: None

None

Lamp-Puppet-test-nsg
southcentralus

ngarm
southcentralus

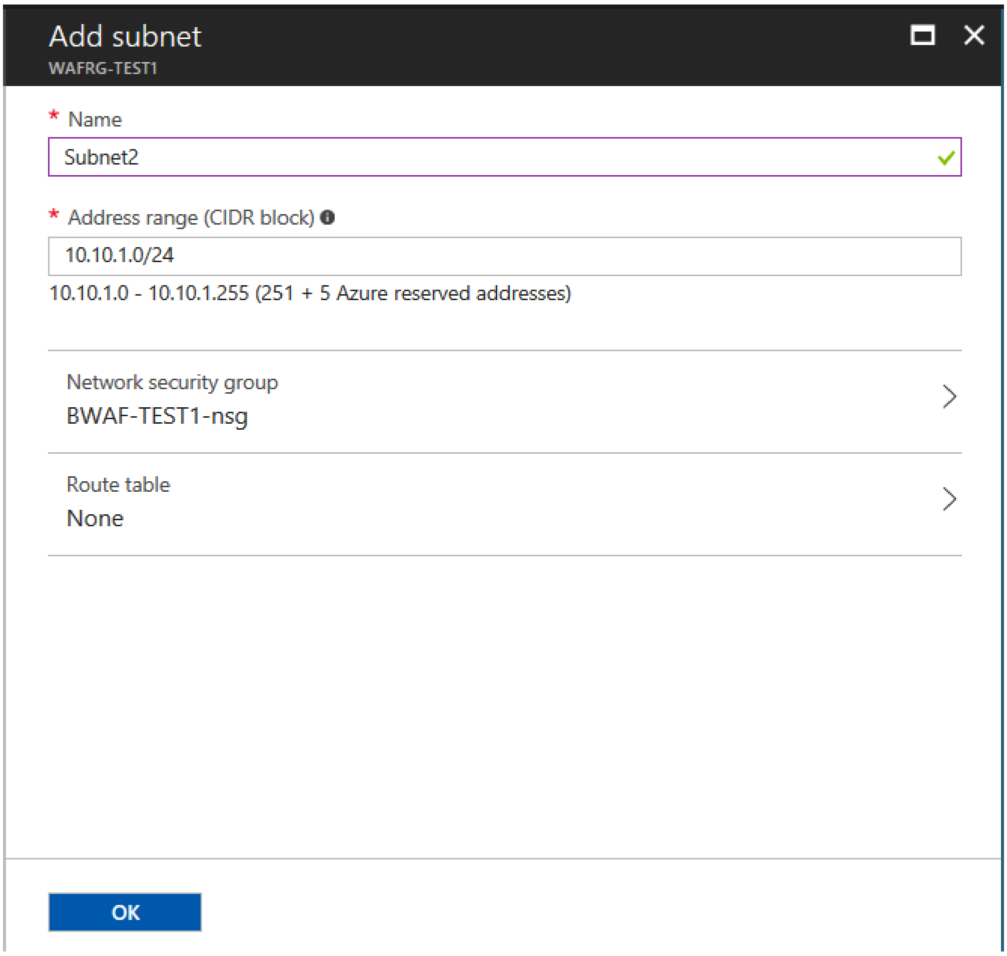
aravindan-lamp-nsg
southcentralus

testing-puppet-nsg
southcentralus

ara-puppet-nsg
southcentralus

BWAF-TEST1-nsg
southcentralus

BWAF-TEST2-nsg
southcentralus



* Name: Subnet2

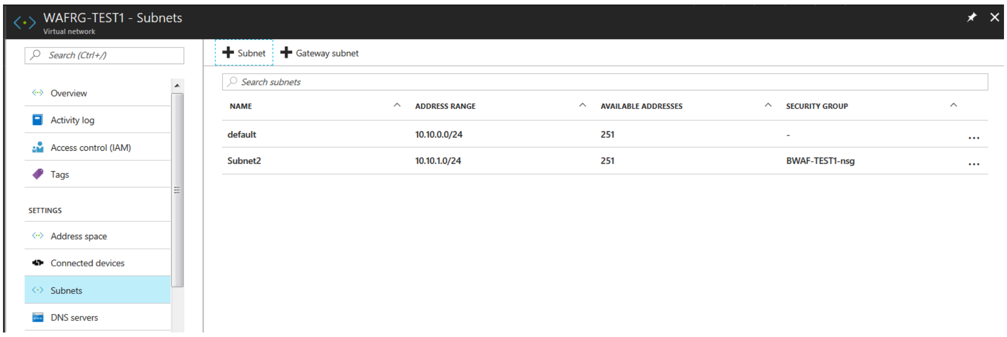
* Address range (CIDR block): 10.10.1.0/24

10.10.1.0 - 10.10.1.255 (251 + 5 Azure reserved addresses)

Network security group: BWAF-TEST1-nsg

Route table: None

6. The new subnet gets displayed in the **Subnets** list.



NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
default	10.10.0.0/24	251	-
Subnet2	10.10.1.0/24	251	BWAF-TEST1-nsg

To configure the Barracuda Web Application Firewall with multiple NICs, perform the following steps:

Step 1. Deploy the Barracuda Web Application Firewall Instance

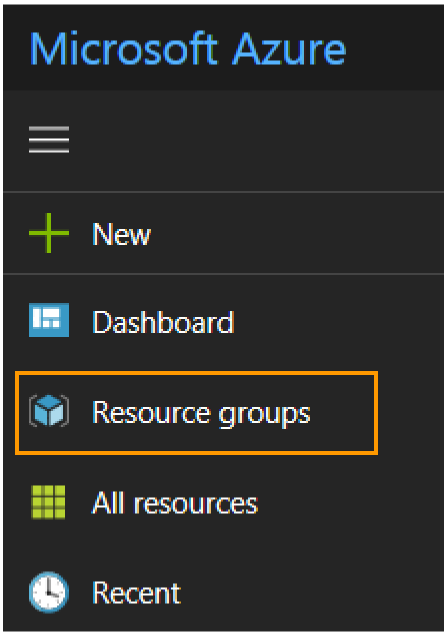
Follow the steps mentioned in Deploying and Provisioning the Barracuda Web Application Firewall in the New Microsoft Azure Management Portal or Deploying and Provisioning the Barracuda Web Application Firewall in the Classic Microsoft Azure Management Portal.

Step 2. Set the Private IP Address of the Instance to Static

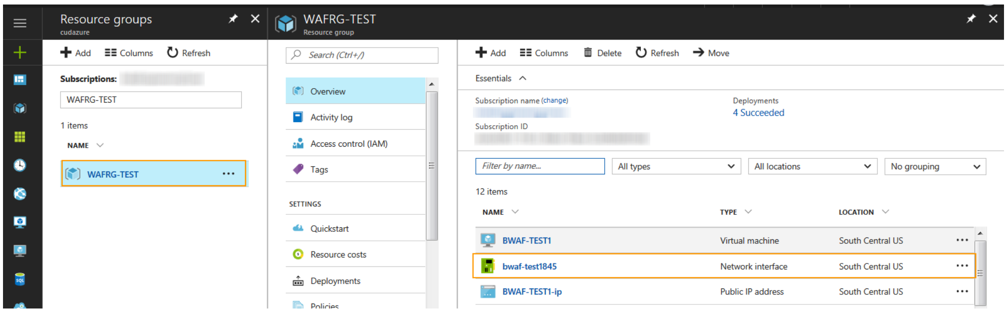
After the instance is deployed, set the private IP address to static by following the steps below:

> The IP address should be changed to static to ensure that the system retains the same IP address even after the system reboots.

1. In the Microsoft Azure portal, click **Resource groups** on the left panel.



2. In the **Resource groups** list, locate and click on the resource group to which the Barracuda Web Application Firewall instance is associated.
3. On the **Resource groups** page, select the network interface (NIC) of the deployed Barracuda Web Application Firewall instance.



Subscriptions: [redacted]

WAFRG-TEST

1 items

NAME
WAFRG-TEST

Subscription name (change) [redacted]

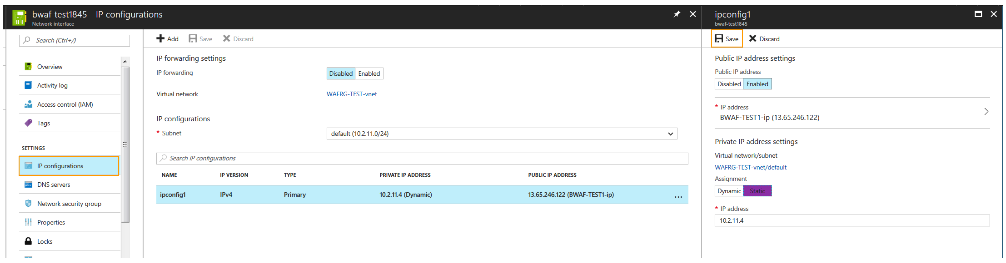
Subscription ID [redacted]

Deployments
4 Succeeded

12 items

NAME	TYPE	LOCATION
BWAF-TEST1	Virtual machine	South Central US
bwaf-test1845	Network interface	South Central US
BWAF-TEST1-ip	Public IP address	South Central US

4. On the instance Network interface page, select **IP configuration** under **Settings**.
5. Select the **Private IP Address** under **IP configurations**.
6. Set **Assignment** to **Static** under **Private IP address settings** and click **Save**.



IP forwarding settings

IP forwarding: Disabled | Enabled

Virtual network: WAFRG-TEST-vnet

IP configurations

* Subnet: default (10.2.11.0/24)

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
ipconfig1	IPv4	Primary	10.2.11.4 (Dynamic)	13.65.246.122 (BWAF-TEST1-ip)

Public IP address settings

Public IP address: Disabled | Enabled

* IP address: BWAF-TEST1-ip (13.65.246.122)

Private IP address settings

Virtual network/subnet: WAFRG-TEST-vnet/default

Assignment: Dynamic | Static

* IP address: 10.2.11.4

Step 3. Create a Network Interface (NIC)

By default, the Barracuda Web Application Firewall instance is deployed with a single NIC. You can add an additional NIC for LAN either through the Azure Portal or Azure CLI.

Create a NIC Using the Azure Portal

1. Log into the Microsoft Azure portal.
2. Click **Marketplace** in the left panel and type `Network Interface` in the **Search Everything** field.
3. Select **Microsoft Network interface** from the search results.
4. On the **Network interface** page, click **Create**.
5. On the **Create network interface** page:
    1. **Name**: Enter a name for the network interface. Example: LAN
    2. **Virtual network**: Select the virtual network for the network interface. Ensure that the virtual network exists in the same subscription and location as that of the network interface.
    3. **Subnet**: Select a subnet within the virtual network.
    4. **Private IP address assignment**: Set to **Static**.
    5. **Private IP address**: Enter an IP address that belongs to the configured subnet.
    6. **Network security group**: Select an existing network security group, or create a network security group.
    7. **Subscription**: Select the subscription from the drop-down list.
    8. **Resource group**: Select **Use existing** and select the resource group to which the Barracuda Web Application Firewall instance is associated.
    9. **Location**: Select the location. Ensure that the network interface location and the location specified for the Barracuda Web Application Firewall instance are the same.
6. Click **Create**.

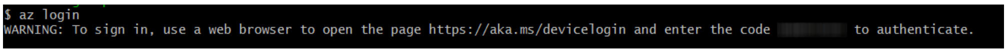
Creating a NIC Using the Azure CLI

To create a network interface using the Azure CLI, perform the steps below:

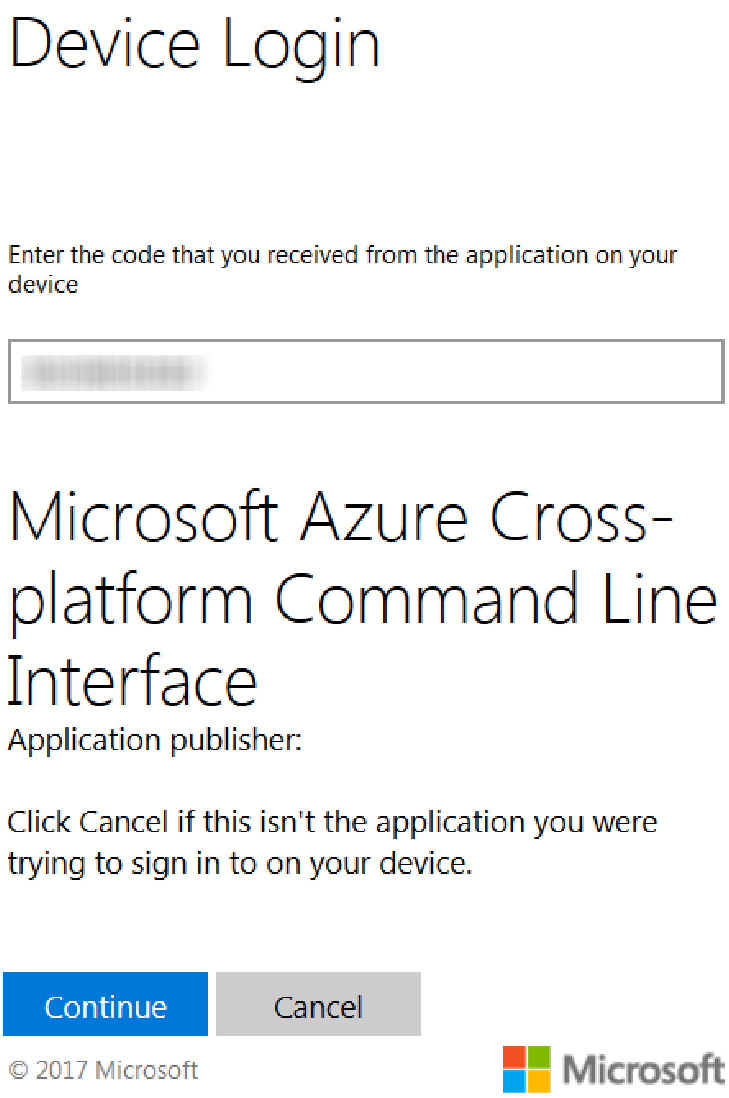
1. Install Azure CLI by following the steps mentioned in Install Azure 2.0 CLI.
2. To authenticate to your Azure account, run the Azure login command and follow the instructions.

    az login

    This displays a message as: “*To sign in, use a web browser to open the page https://aka.ms/devicelogin and enter the code ********* to authenticate.*”

    ```
    $ az login
    WARNING: To sign in, use a web browser to open the page https://aka.ms/devicelogin and enter the code [redacted] to authenticate.
    ```
3. Copy the URL and paste it in the web browser.
4. Enter the **Code** in the text field and click **Continue**.



Device Login

Enter the code that you received from the application on your device

[redacted]

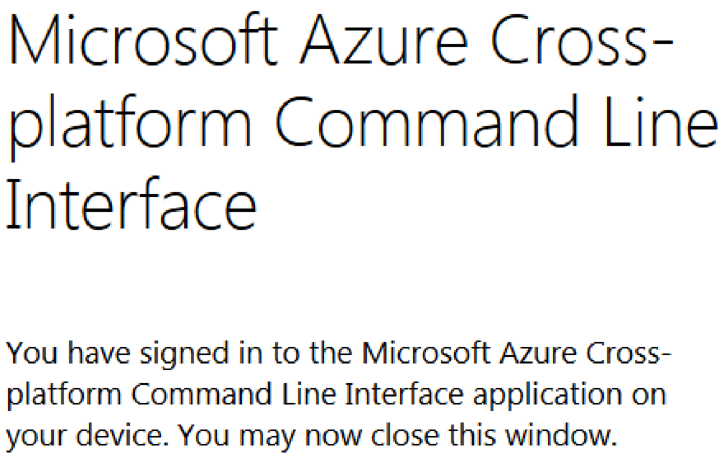
Microsoft Azure Cross-platform Command Line Interface

Application publisher:

Click Cancel if this isn't the application you were trying to sign in to on your device.

© 2017 Microsoft

5. Enter your Microsoft account username and password.
6. After successful authentication, you can use the Azure CLI to perform actions on your Azure account.



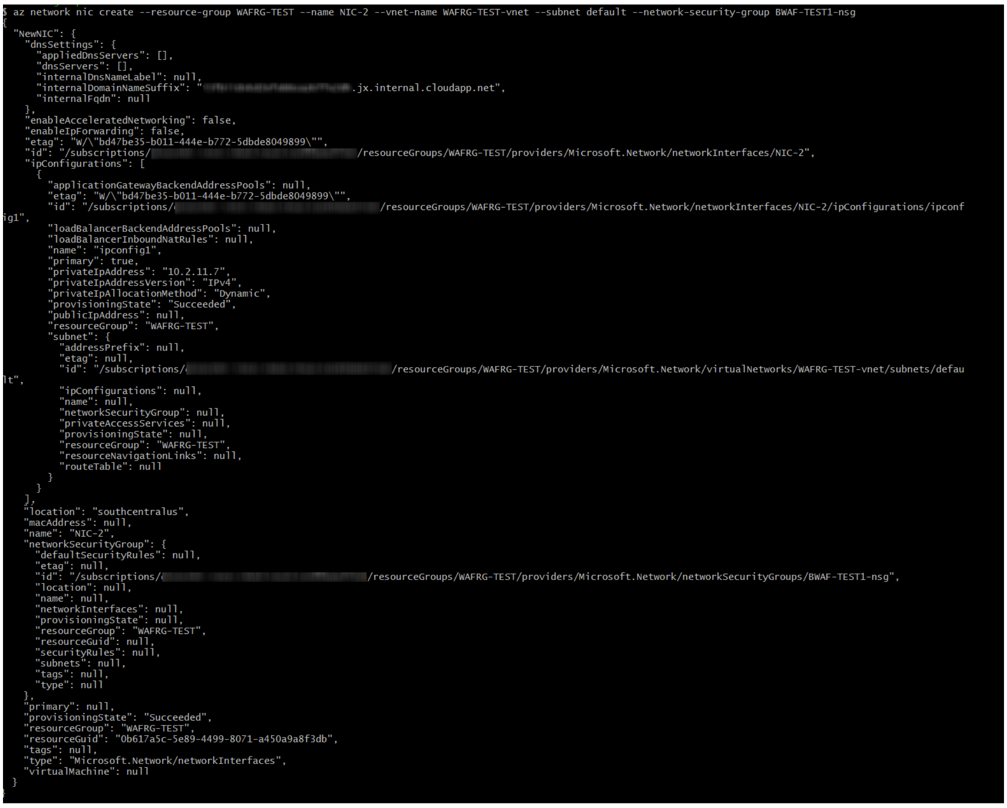
Microsoft Azure Cross-platform Command Line Interface

You have signed in to the Microsoft Azure Cross-platform Command Line Interface application on your device. You may now close this window.

7. Run the following command to create a NIC:

   az network nic create --resource-group <*Resource group name to which your Barracuda Web Application Firewall instance is associated*> **--name** <*Name for the new NIC*> **--vnet-name** <*Name of the virtual network to which this network interface needs to be created*> **--subnet** <*Name of the subnet*> **--network-security-group** <*Name of the network security group*>

   Example: az network nic create --resource-group WAFRG-TEST --name NIC-2 --vnet-name WAFRG-TEST-vnet --subnet default --network-security-group BWAF-TEST1-nsg

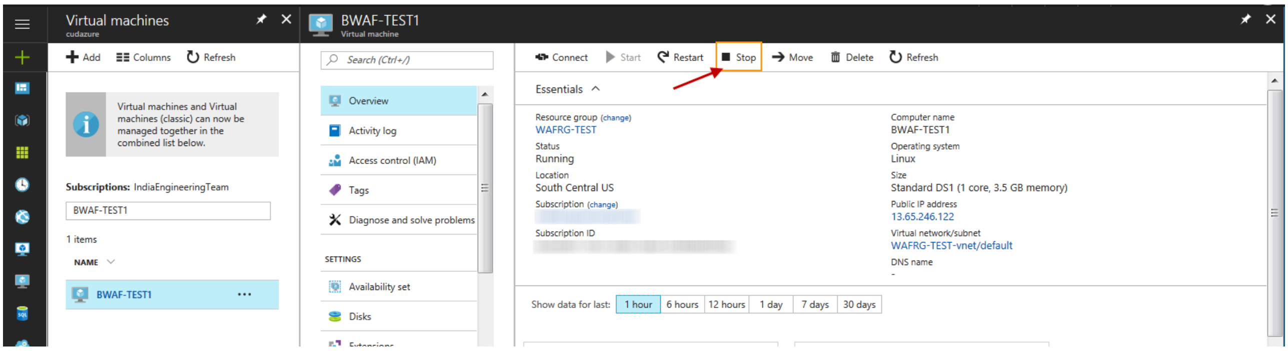


```
$ az network nic create --resource-group WAFRG-TEST --name NIC-2 --vnet-name WAFRG-TEST-vnet --subnet default --network-security-group BWAF-TEST1-nsg
{
  "NewNIC": {
    "dnsSettings": {
      "appliedDnsServers": [],
      "dnsServers": [],
      "internalDnsNameLabel": null,
      "internalDomainNameSuffix": "[redacted].jx.internal.cloudapp.net",
      "internalFqdn": null
    },
    "enableAcceleratedNetworking": false,
    "enableIpForwarding": false,
    "etag": "W/\"bd47be35-b011-444e-b772-5dbde8049899\"",
    "id": "/subscriptions/[redacted]/resourceGroups/WAFRG-TEST/providers/Microsoft.Network/networkInterfaces/NIC-2",
    "ipConfigurations": [
      {
        "applicationGatewayBackendAddressPools": null,
        "etag": "W/\"bd47be35-b011-444e-b772-5dbde8049899\"",
        "id": "/subscriptions/[redacted]/resourceGroups/WAFRG-TEST/providers/Microsoft.Network/networkInterfaces/NIC-2/ipConfigurations/ipconf
ig1",
        "loadBalancerBackendAddressPools": null,
        "loadBalancerInboundNatRules": null,
        "name": "ipconfig1",
        "primary": true,
        "privateIpAddress": "10.2.11.7",
        "privateIpAddressVersion": "IPv4",
        "privateIpAllocationMethod": "Dynamic",
        "provisioningState": "Succeeded",
        "publicIpAddress": null,
        "resourceGroup": "WAFRG-TEST",
        "subnet": {
          "addressPrefix": null,
          "etag": null,
          "id": "/subscriptions/[redacted]/resourceGroups/WAFRG-TEST/providers/Microsoft.Network/virtualNetworks/WAFRG-TEST-vnet/subnets/defau
lt",
          "ipConfigurations": null,
          "name": null,
          "networkSecurityGroup": null,
          "privateAccessServices": null,
          "provisioningState": null,
          "resourceGroup": "WAFRG-TEST",
          "resourceNavigationLinks": null,
          "routeTable": null
        }
      }
    ],
    "location": "southcentralus",
    "macAddress": null,
    "name": "NIC-2",
    "networkSecurityGroup": {
      "defaultSecurityRules": null,
      "etag": null,
      "id": "/subscriptions/[redacted]/resourceGroups/WAFRG-TEST/providers/Microsoft.Network/networkSecurityGroups/BWAF-TEST1-nsg",
      "location": null,
      "name": null,
      "networkInterfaces": null,
      "provisioningState": null,
      "resourceGroup": "WAFRG-TEST",
      "resourceGuid": null,
      "securityRules": null,
      "subnets": null,
      "tags": null,
      "type": null
    },
    "primary": null,
    "provisioningState": "Succeeded",
    "resourceGroup": "WAFRG-TEST",
    "resourceGuid": "0b617a5c-5e89-4499-8071-a450a9a8f3db",
    "tags": null,
    "type": "Microsoft.Network/networkInterfaces",
    "virtualMachine": null
  }
}
```

Step 4. Add the LAN Network Interface to the Barracuda Web Application Firewall Instance

To add the created network interface to the Barracuda Web Application Firewall instance, perform the following steps:

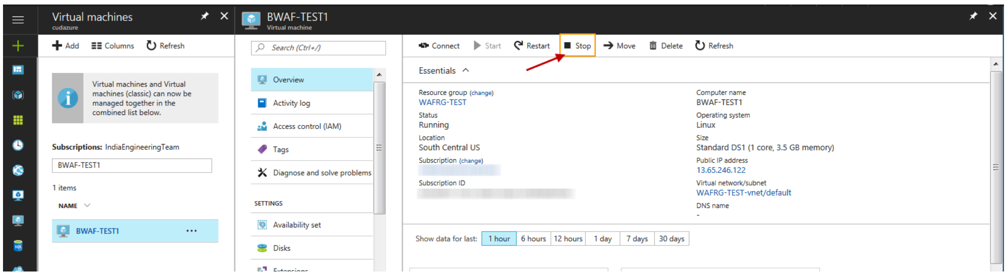
1. Log into the Microsoft Azure Portal.
2. Click **Virtual machines** in the left panel.



Resource group (change)
WAFRG-TEST
Status
Running
Location
South Central US
Subscription (change)
[redacted]
Subscription ID
[redacted]

Computer name
BWAF-TEST1
Operating system
Linux
Size
Standard DS1 (1 core, 3.5 GB memory)
Public IP address
13.65.246.122
Virtual network/subnet
WAFRG-TEST-vnet/default
DNS name
-

3. In the **Virtual machines** list, click on the virtual machine to which the network interface needs to be added.
4. Click **Stop** to shut down the virtual machine.



Resource group (change)
WAFRG-TEST
Status
Running
Location
South Central US
Subscription (change)
[redacted]
Subscription ID
[redacted]

Computer name
BWAF-TEST1
Operating system
Linux
Size
Standard DS1 (1 core, 3.5 GB memory)
Public IP address
13.65.246.122
Virtual network/subnet
WAFRG-TEST-vnet/default
DNS name

5. After the virtual machine has stopped, go to the Microsoft Azure Command Line Interface, and run the following command:

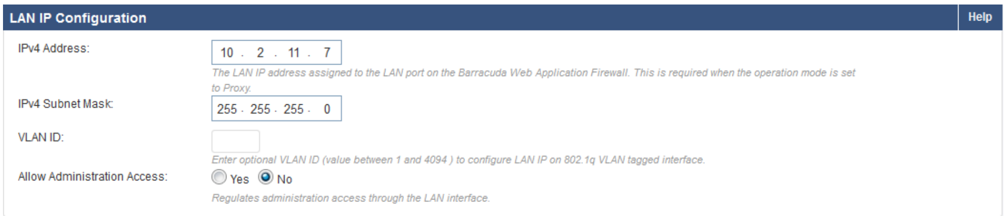
   az vm nic add --output json --vm-name <*Name of the Barracuda Web Application Firewall instance to which the network interface needs to added*> **--resource-group** <*Name of the resource group*> **--nics** <*Name of the network interface that needs to be added to the instance*>

   Example: az vm nic add --output json --vm-name BWAF-TEST1 --resource-group WAFRG-TEST --nics NIC-2

Step 5. Configure the LAN IP Address

The private IP address of the new NIC should be configured as the LAN IP address in the **BASIC > IP Configuration** page.

1. Log into the Barracuda Web Application Firewall web interface.
2. Go to the **BASIC > IP Configuration** page.
3. In the **LAN IP Configuration** section:
    1. **IPv4 Address**: Enter the IP address of the second NIC that was added to the instance.
    2. **IPv4 Subnet Mask**: Enter the netmask associated with the IP address
    3. **Allow Administration Access**: Set to **No** to allow administration access.
4. Click **Save**.



IPv4 Address: 10 . 2 . 11 . 7

The LAN IP address assigned to the LAN port on the Barracuda Web Application Firewall. This is required when the operation mode is set to Proxy.

IPv4 Subnet Mask: 255 . 255 . 255 . 0

VLAN ID:

Enter optional VLAN ID (value between 1 and 4094) to configure LAN IP on 802.1q VLAN tagged interface.

Allow Administration Access: ○ Yes ● No

Regulates administration access through the LAN interface.

Figures