Reserved, Static and Public IP Addresses in the Azure Cloud using ASM

https://campus.barracuda.com/doc/47579397/

By default, a VM in the Azure cloud uses the hostname and IP address assigned to the cloud service the VM resides in. Whereas the hostname does not change as long as the cloud service exists, the IP address is allocated dynamically and changes every time all VMs in the cloud service are stopped. This may also occur during Azure maintenance windows if your VMs are not assigned an availability set. Azure allows you to reserve both the internal IP addresses and external cloud service IP address. Reserved IP addresses are limited to five per subscription.

In this article:

Static Internal IP Addresses for the VM

In many cases, it is easier to use a static internal IP address than to use the default DHCP interface with dynamic IP addresses. If you want to deploy an HA cluster, you must use static internal IP addresses and static network interfaces on the Barracuda NextGen Firewall F-Series for HA sync to operate. Static IP addresses are also required for Barracuda NextGen Control Centers in Azure and recommended for Azure NextGen F-Series Firewalls managed by an Azure NextGen Control Center. You can assign static internal IP addresses by deploying the NextGen Firewall F-Series via the new Azure portal, or by changing the IP address for existing VMs via Azure PowerShell.

> The Azure virtual machine will automatically reboot when assigning the static IP address.

Before you Begin

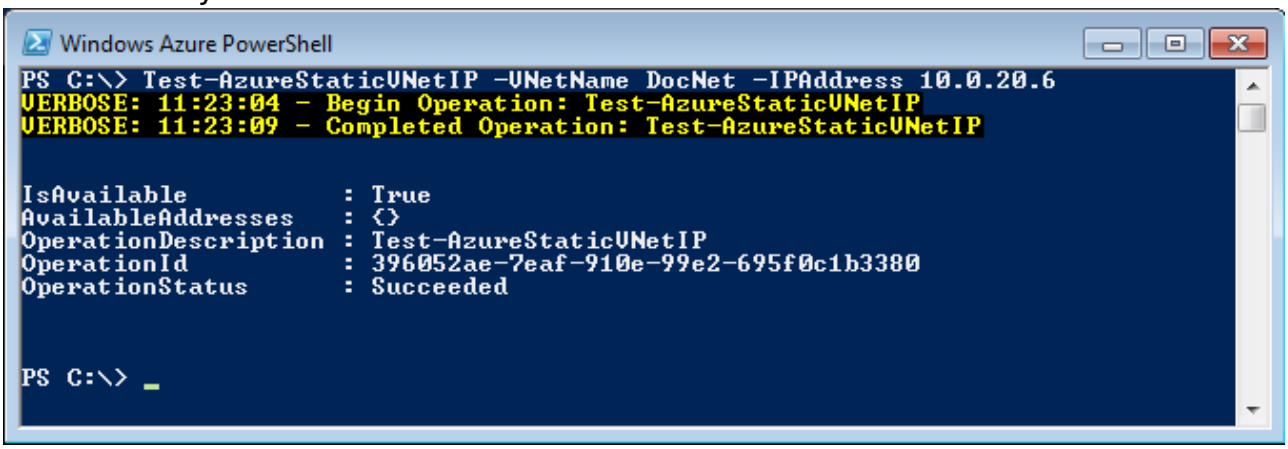
- Deploy a F-Series Firewall VM. For more information, see Microsoft Azure Deployments using Azure Service Manager (ASM)
- Install Azure PowerShell version 0.9.8 or higher.

Step 1. Reserve a Static Internal IP Address

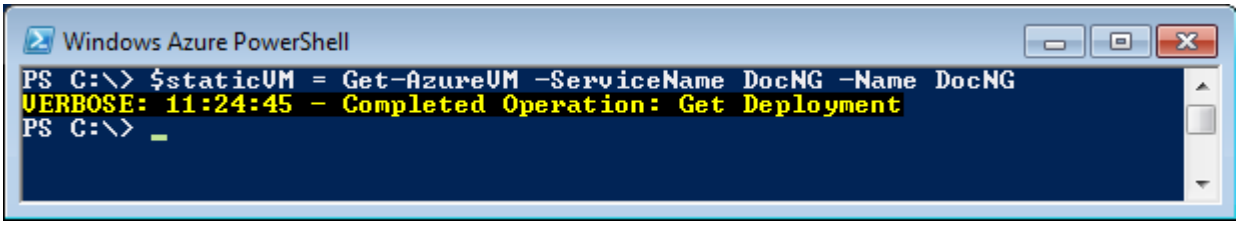
By default, the internal IP addresses are assigned via DHCP in the internal Azure network. Choose a free IP address in the Virtual Network for the Barracuda NextGen Firewall F-Series. It must be different from the IP addresses already assigned to the virtual machine.

1. Open a Windows Azure PowerShell.

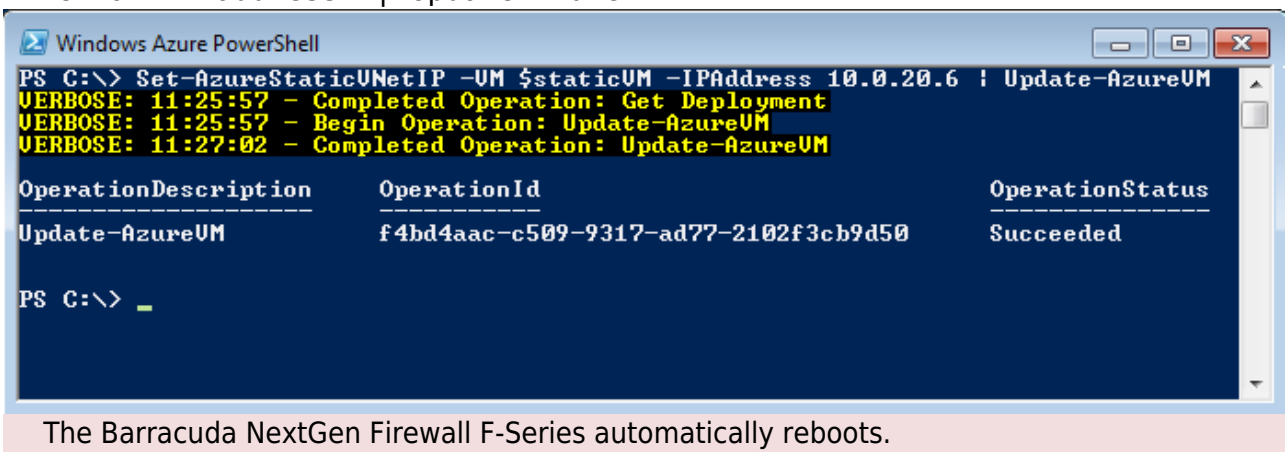
2. Check if the chosen IP address is available by entering:
   `Test-AzureStaticVNetIP -VNetName <your Azure virtual network name> -IPAddress <your chosen static internal IP address>`



3. Save the virtual machine to a local variable.
   `$staticVM = Get-AzureVM -ServiceName <Cloud Service name of your NG> -Name <virtual machine name>`

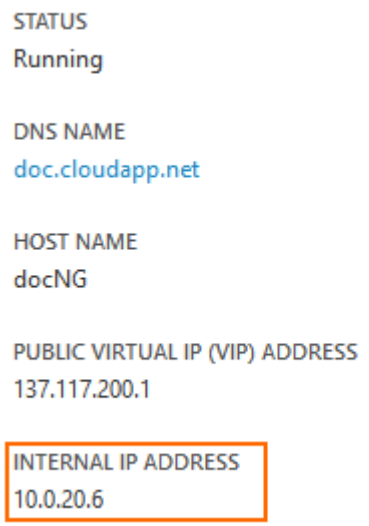


4. Change the internal IP address of the virtual machine from dynamic to static.
   `Set-AzureStaticVNetIP -VM $staticVM -IPAddress <your chosen static internal IP address> | Update-AzureVM`



The Barracuda NextGen Firewall F-Series automatically reboots.

The Barracuda NextGen Firewall F-Series VM is now using a static internal IP address:



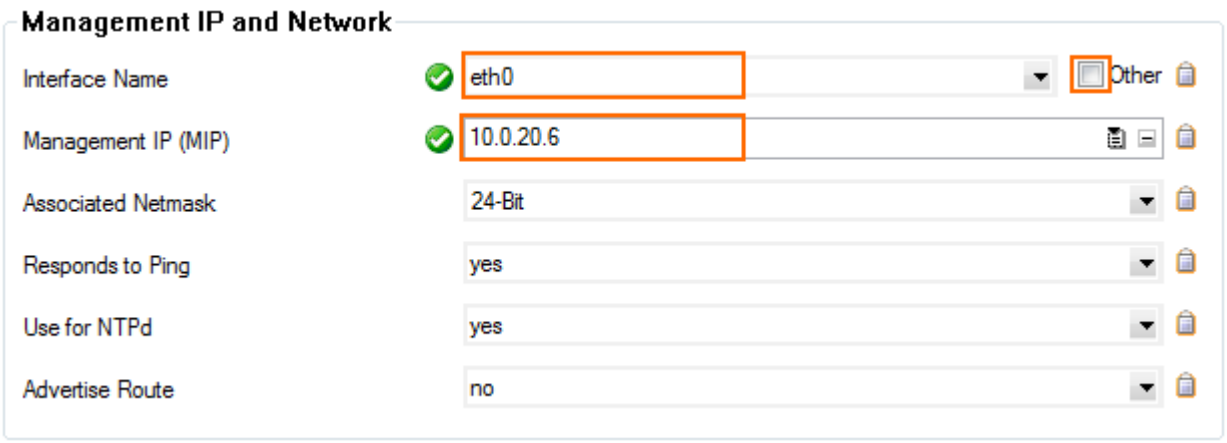
Step 2. Change the Network Configuration to Use the Static Internal IP Address

Change the network configuration to use a static network interface.

Step 2.1 Reconfigure the Network Interface

Change the network interface type from dynamic to static.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. In the left menu, click on **xDSL/DHCP/ISDN**.
3. Click **Lock**.
4. Delete the **DHCP01** entry in the **DHCP Links** list.
5. Select **No** from the **DHCP Enabled** dropdown list.
6. Click **Send Changes**.
7. In the left menu, click on **IP Configuration**.
8. In the **Management IP and Network** section in the **Interface Name** line, untick the **Other** checkbox.
9. Select **eth0** from the **Interface Name** list.
10. Enter the static internal IP address from Step 1 as the **Management IP (MIP)**. E.g., `10.0.20.6`

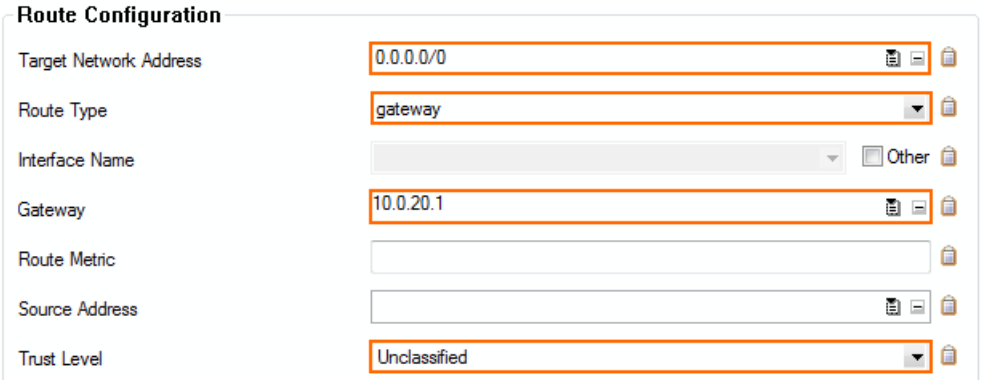


Step 2.2 Create the Default Route

Add the default route. The default gateway in Azure subnets is always the first IP in the subnet. E.g., 10.0.20.1 if the subnet is 10.0.20.0/24

1. In the left menu, click on **Routing**.
2. Click **+** in the **Routes** table and configure the following settings:
   - **Target Network Address** – Enter `0.0.0.0/0`
   - **Route Type** – Select **gateway**.
   - **Gateway** – Enter the first IP address of the subnet the firewalls reside in. E.g., `10.0.20.1` if the IP addresses of the firewalls are 10.0.20.6 and 10.0.20.7
   - **Trust Level** – Select **Unclassified**.

     Do not set the **Trust Level** to **Trusted**.



3. Click **OK**.
4. Click **Send Changes** and **Activate**.

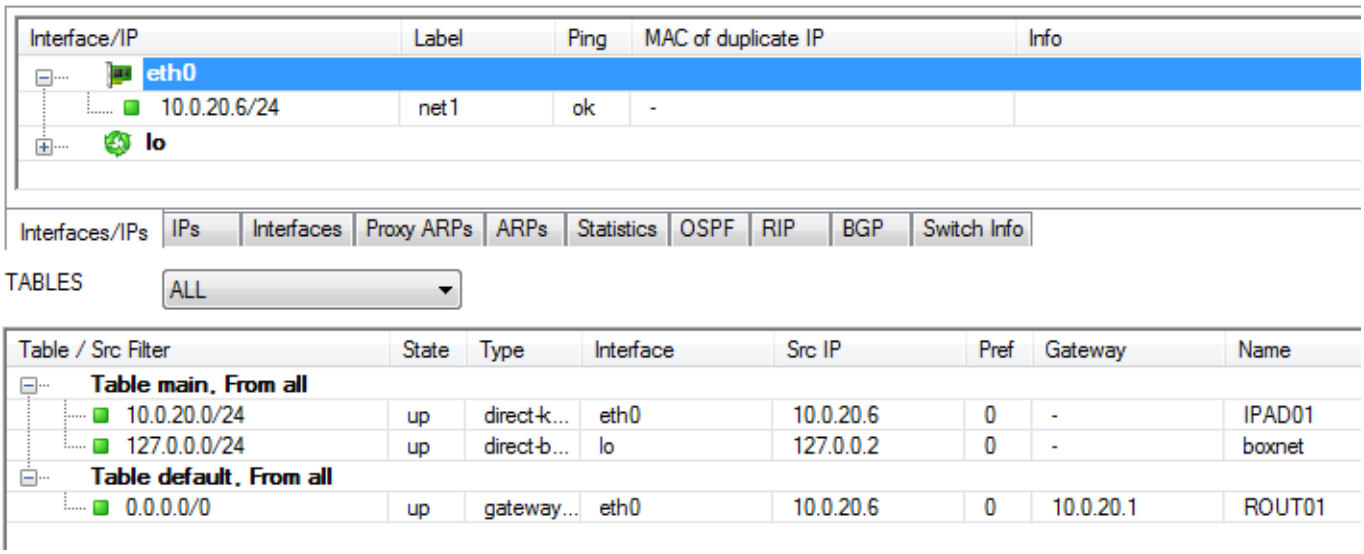
Step 2.3 Activate the Network Changes

Activate the changes to the network configuration.

1. Go to **CONTROL > Box**.
2. In the **Network** section of the left menu, click on **Activate new network configuration**.

3. Click **Failsafe**.

Open the **CONTROL > Network** page. Your interface and IP address are now static.



Reserved IP Addresses (RIP) for the Cloud Service

You can use up to five Reserved IP addresses (RIP) per subscription and assign them to your cloud services. You cannot add a RIP to an already existing cloud service or when creating a cloud service using the web portal. You must create the cloud service via an Azure PowerShell script.

Modify the example Azure deployment script below:

```
# # Example Deployment Script with Reserved IP address # $subscription =
"Pay-As-You-Go" $vmname = "BNG" $pwd = "YOURPASSWORD" $instanceSize = "Small"
$cloudService = "BNGCloudService" $location = "West Europe" $storageAccount
="BNGStorage" $reservedIPname = "BNGRIP" # Get latest Barracuda NextGen
Firewall F-Series ImageName from Azure # IMPORTANT: The following commands
must all be placed on one line! $image = Get-AzureVMImage | where {
$_.ImageFamily -Match "Barracuda NextGen Firewall F-Series*"} | sort
PublishedDate -Descending | select -ExpandProperty ImageName -First 1 #
Create a new Reserved IP $reservedIP = New-AzureReservedIP -ReservedIPName
$reservedIPname -Label $reservedIPname -Location $location #Set your Azure
Subscription Set-AzureSubscription -SubscriptionName $subscription -
CurrentStorageAccountName $storageAccount # Create VM Config and set
Password. The user is ignored # IMPORTANT: The following commands must all be
placed on one line! $vm1 = New-AzureVMConfig -Name $vmname -InstanceSize
$instanceSize -Image $image | Add-AzureProvisioningConfig -Linux -LinuxUser
```

```
"azureuser" -Password $pwd # Create VM and use the new Reserved IP New-
AzureVM -ServiceName $cloudService -VM $vm1 -ReservedIPName $reservedIPName -
Location $location
```

Public Instance Level IP Addresses (PIP)

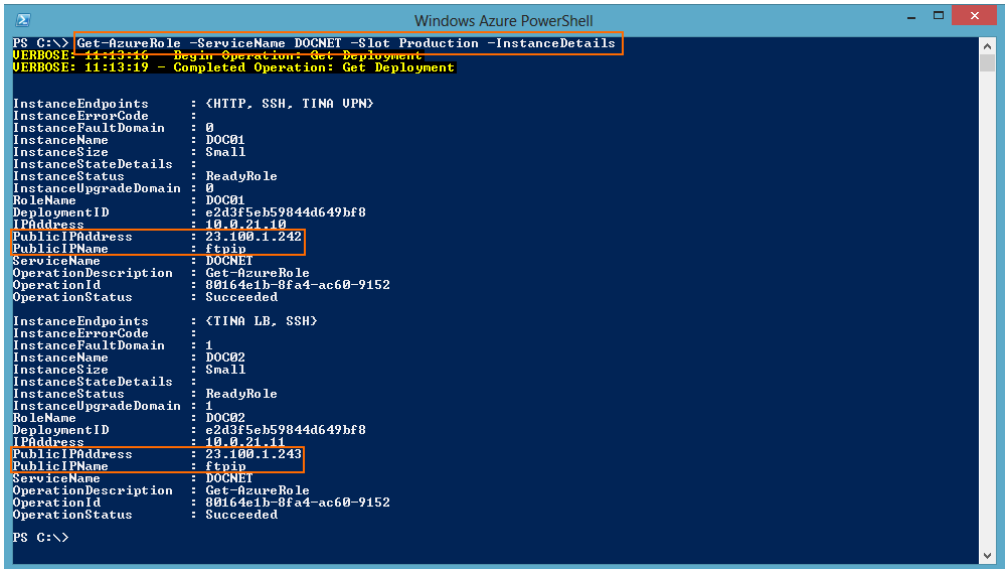
A Public Instance Level IP address (PIP) is directly assigned to your Barracuda NextGen Firewall F-Series, rather than to the cloud service. This additional IP address allows you to directly access the Barracuda NextGen Firewall F-Series without going through the VIP and endpoints of the cloud service, thereby removing the restriction of only being able to use TCP and UDP protocols. All IP-based protocols can be used (ICMP,ESP,...). When a VM is assigned a PIP, all traffic is sent by default using the PIP as the source IP address. Only connections using the VIP to connect to the VM use the VIP address as the source IP address. You must use Azure PowerShell cmdlets to assign a PIP to a VM. You can use up to five PIPs per Azure subscription.

Assign a Public Instance Level IP address to your existing Barracuda NextGen Firewall F-Series VM:

```
# IMPORTANT: The following commands must all be placed on one line! Get-
AzureVM -ServiceName YOUR-CLOUD-SERVICE-NAME -Name YOUR-BARRACUDA-NG-FIREWALL
| Set-AzurePublicIP -PublicIPName CHOOSE-A-NAME | Update-AzureVM
```

The Barracuda NextGen F-Series Firewalls are now reachable via their PIP. You can get PIP information on the instances by:

```
Get-AzureRole -ServiceName <your> -Slot -InstanceDetails
```



Figures

1. AzureHA01.png
2. AzureHA02.png
3. AzureHA03.png
4. AzureHA04.png
5. AzureHA08.png
6. Azure_default_route.png
7. AzureHA11.png
8. PIP03.png