How to Configure a High Availability Cluster in Azure

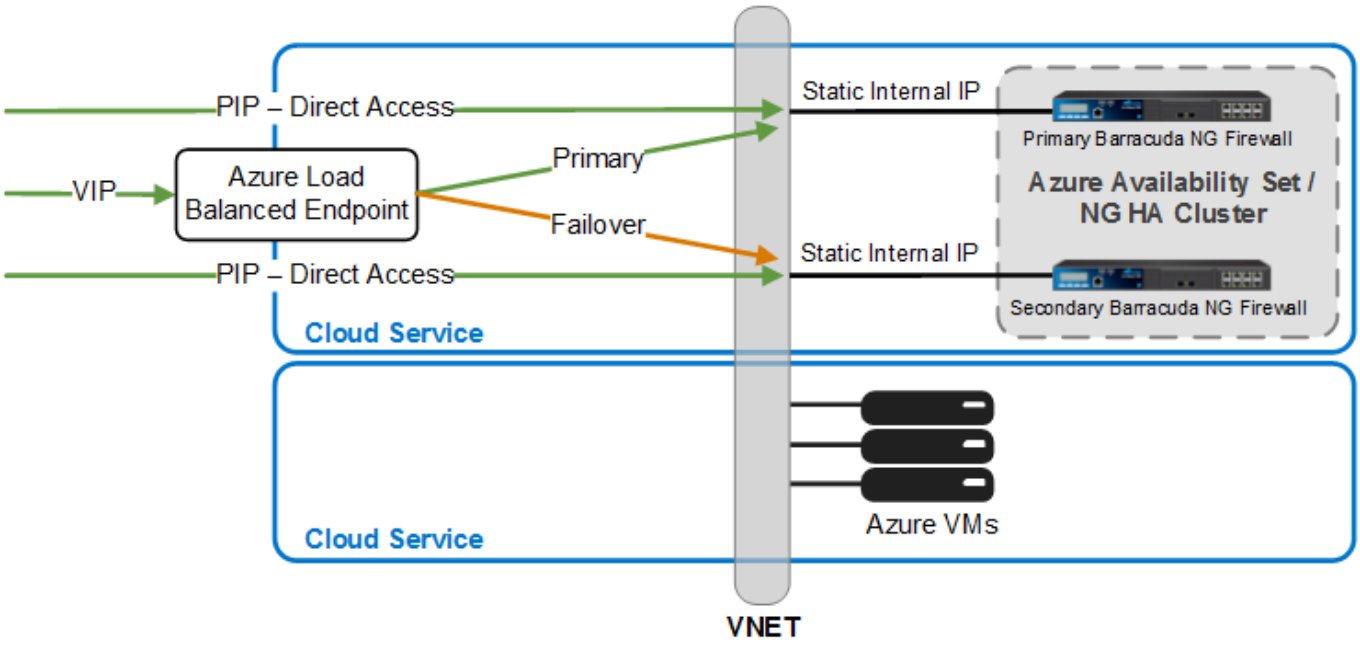
https://campus.barracuda.com/doc/41116373/

To safeguard against hardware and software failures in the Azure cloud, use a high availability (HA) setup. The Barracuda NG Firewall units are deployed in an Azure availability set in a cloud service in order to guarantee that both virtual machines are running in different fault domains in the Azure datacenter. To access the NG Firewalls, use the virtual IP of the cloud service and/or individual Public Instance Level IP addresses (PIPs). Both systems are connected to the same Azure virtual network and use static internal IP addresses (DIPs). An Azure load-balanced endpoint (level 4 load balancer) can be used to offer TCP- and UDP-based services on the VIP. PIPs allow direct access to the services on the NG Firewall VM for all IP-based protocols.

Azure (Load-balanced) Endpoints can only be used for TCP/UDP-based services. All other IP protocols (ICMP, ESP,...) are blocked.

You can configure services in the HA cluster in the Azure cloud to use:

1. The public VIP IP address of the cloud service with a load-balanced endpoint for each Internet facing service. PIPs grant management access to both units in the HA cluster. A load-balanced endpoint must be created for each service Port
   If you do not want to use PIPs, you can also exclusively use the VIP for management access and all services running on the NG Firewalls:
   - Create an Endpoint on port TCP/807 to manage the primary NG Firewall.
   - Configure a C2S VPN. You can now reach the static internal IP address of the secondary NG Firewall through the Client-to-Site VPN.
2. Two public facing IP addresses (PIPs). In case of a failover, the remote host must be configured to use the PIP of the secondary unit when the primary host is unreachable.
3. A mix of single VIP and dual external PIP IP addresses.



In this article:

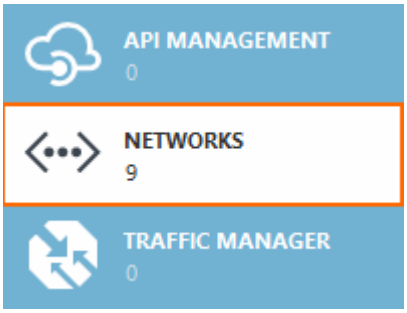
Before you Begin

- Install Windows PowerShell for Azure version 0.7.3.1 or later. (http://azure.microsoft.com/en-us/downloads/)
- You must have two unused Public Instance Level IP addresses in your Azure subscription.

Step 1. Create an Azure Wide Virtual Network

Public Instance Level IPs (PIPs) require a wide Virtual Network (wideVNET). WideVNETs use the *Location* tag instead of the AffinityGroup and cannot be created using the web interface.

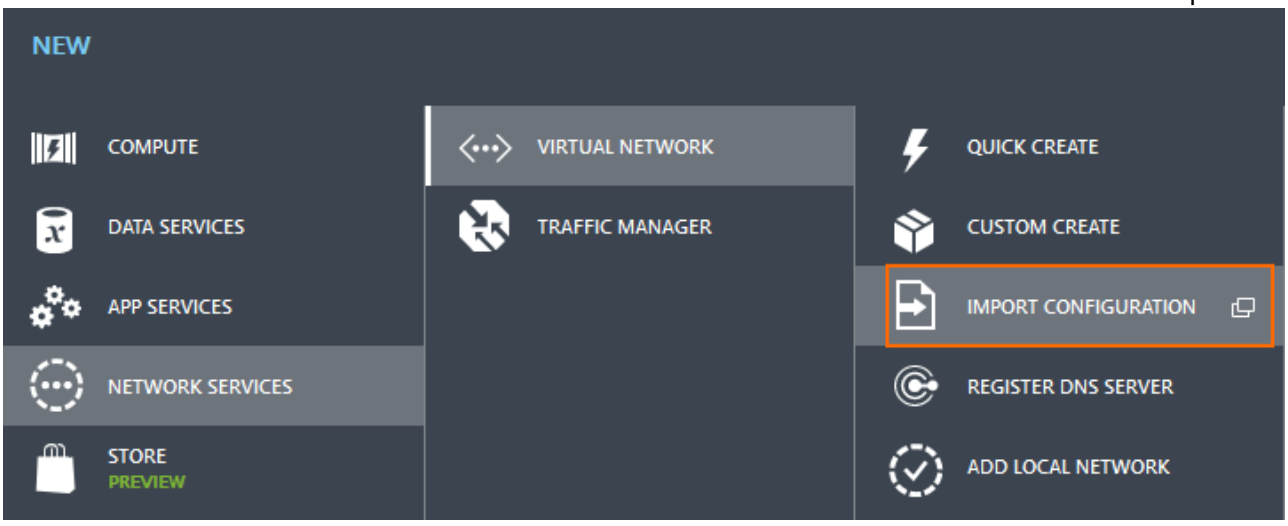
1. Log into your Microsoft Azure Management Portal (https://manage.windowsazure.com).
2. In the left pane, click on **NETWORKS**.



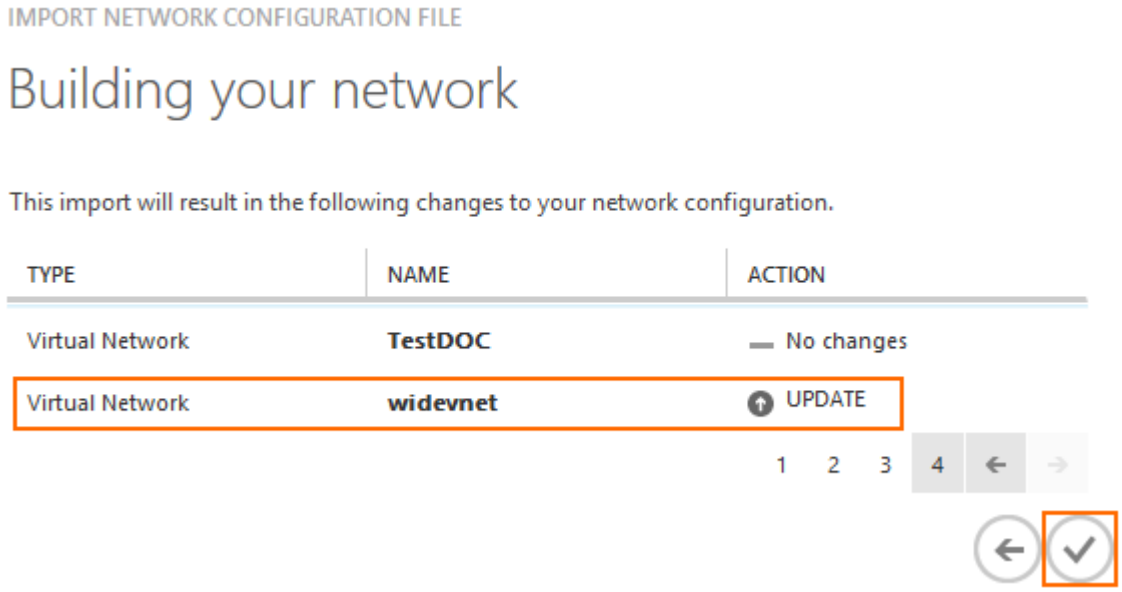
3. Click **EXPORT** in the bottom pane to download the current network configuration as an XML file. You are prompted to save the `NetworkConfig.xml` file.
4. Edit the network configuration XML file and add a definition for the wide Virtual Network. Alternatively, you can also modify an existing Virtual Network.

```
[...]

  <VirtualNetworkSite name="wideVNET" Location="West Europe">
    <Subnets>
      <Subnet name="SubnetWideVNET">
        <AddressPrefix>10.0.21.0/24</AddressPrefix>
      </Subnet>
    </Subnets>
    <AddressSpace>
      <AddressPrefix>10.0.0.0/16</AddressPrefix>
    </AddressSpace>
  </VirtualNetworkSite>

[...]
```

5. In the lower left-hand corner, click **+ NEW > NETWORK SERVICES > VIRTUAL NETWORK > IMPORT CONFIGURATION**. The **IMPORT NETWORK CONFIGURATION FILE** window opens.

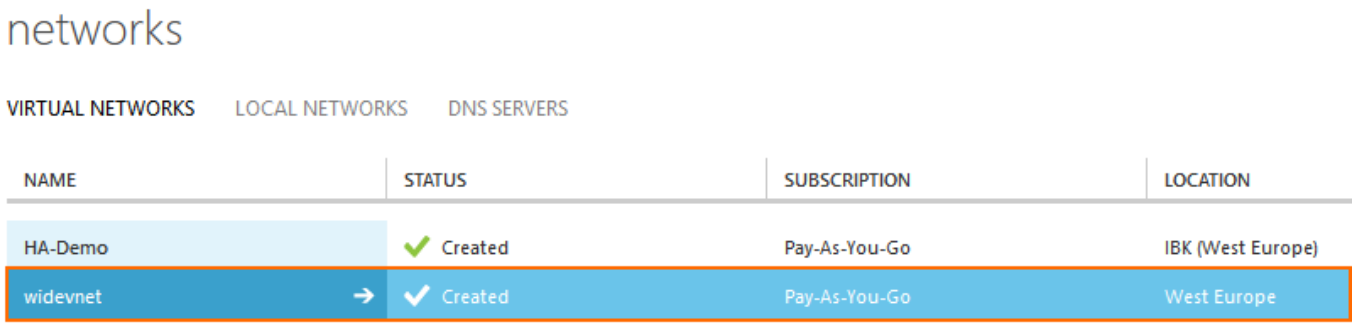


6. Select the modified network configuration XML file and click **Next**.
7. Verify the changes to your Virtual Networks and click **OK**.



8. Click **OK**.

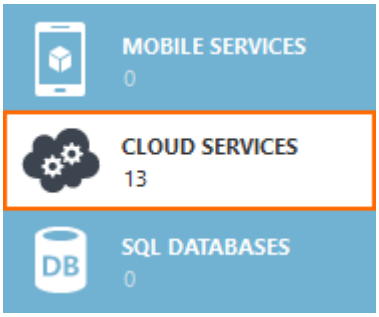
Your wideVNET is now listed in the **NETWORKS** section. You can differentiate between the old Affinity Group-based Virtual Networks and the new Location-based wideVNETs by the missing Affinity Group in the **LOCATION** column.



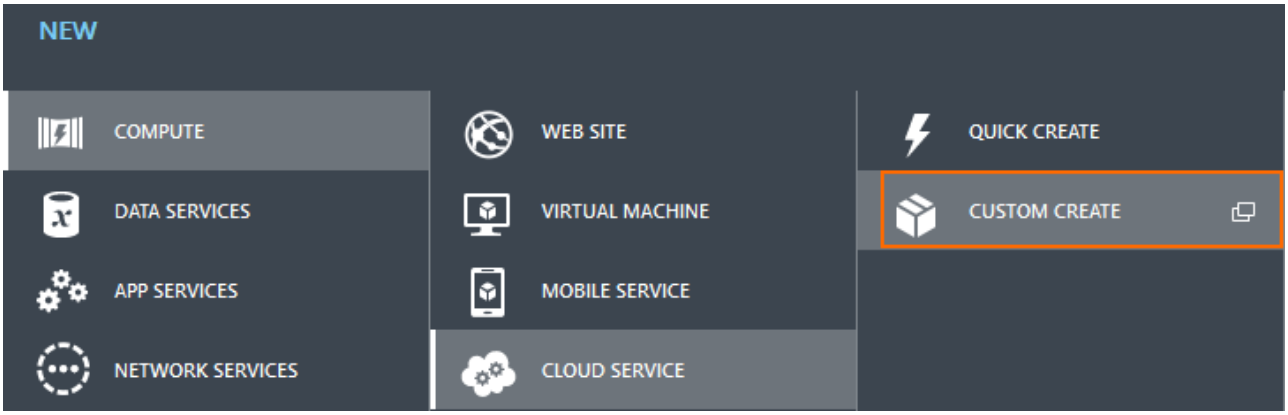
Step 2. Create an Azure Cloud Service

Create a cloud service. The Barracuda NG Firewalls will be deployed in the same cloud service so you can later assign both virtual machines the same Availability Set.

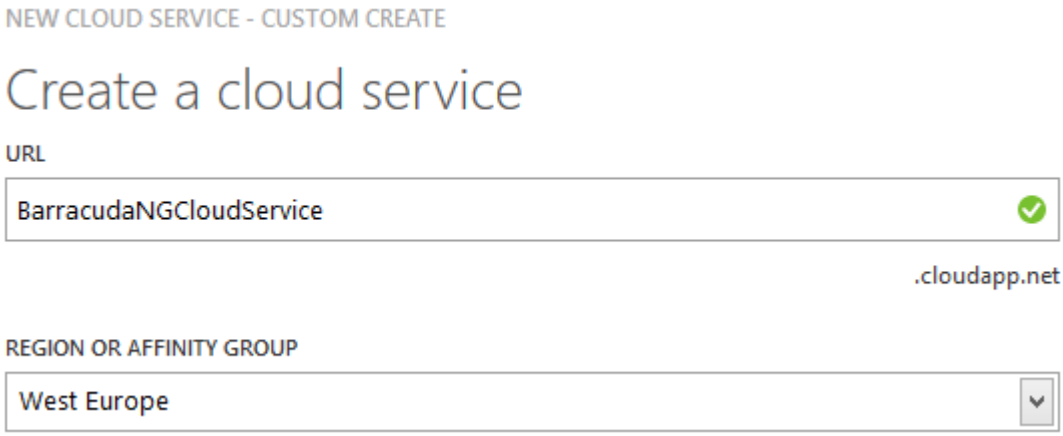
1. Log into your Microsoft Azure Management Portal (https://manage.windowsazure.com).
2. In the left pane, click on **CLOUD SERVICES**.



3. In the lower left-hand corner click **+ NEW > COMPUTE > CLOUD SERVICE > CUSTOM CREATE**.

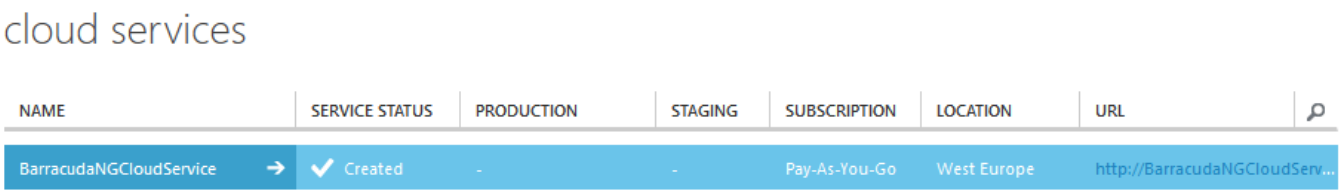


4. Enter the **URL** for the cloud service. E.g., `BarracudaNGCloudService`
5. Select a **REGION OR AFFINITY GROUP** for the cloud service. E.g., `West Europe`



6. Click **OK**.

You now have a cloud service located in the Azure datacenter of your choice.



Step 3. Deploy Two Barracuda NG Firewalls

Deploy two Barracuda NG Firewall Virtual Machines in the Microsoft Azure cloud, using:

- The cloud service created in Step 2.
- The wide Virtual Network created in Step 1.

For more information, see How to Deploy the Barracuda NG Firewall Azure on Microsoft Azure.

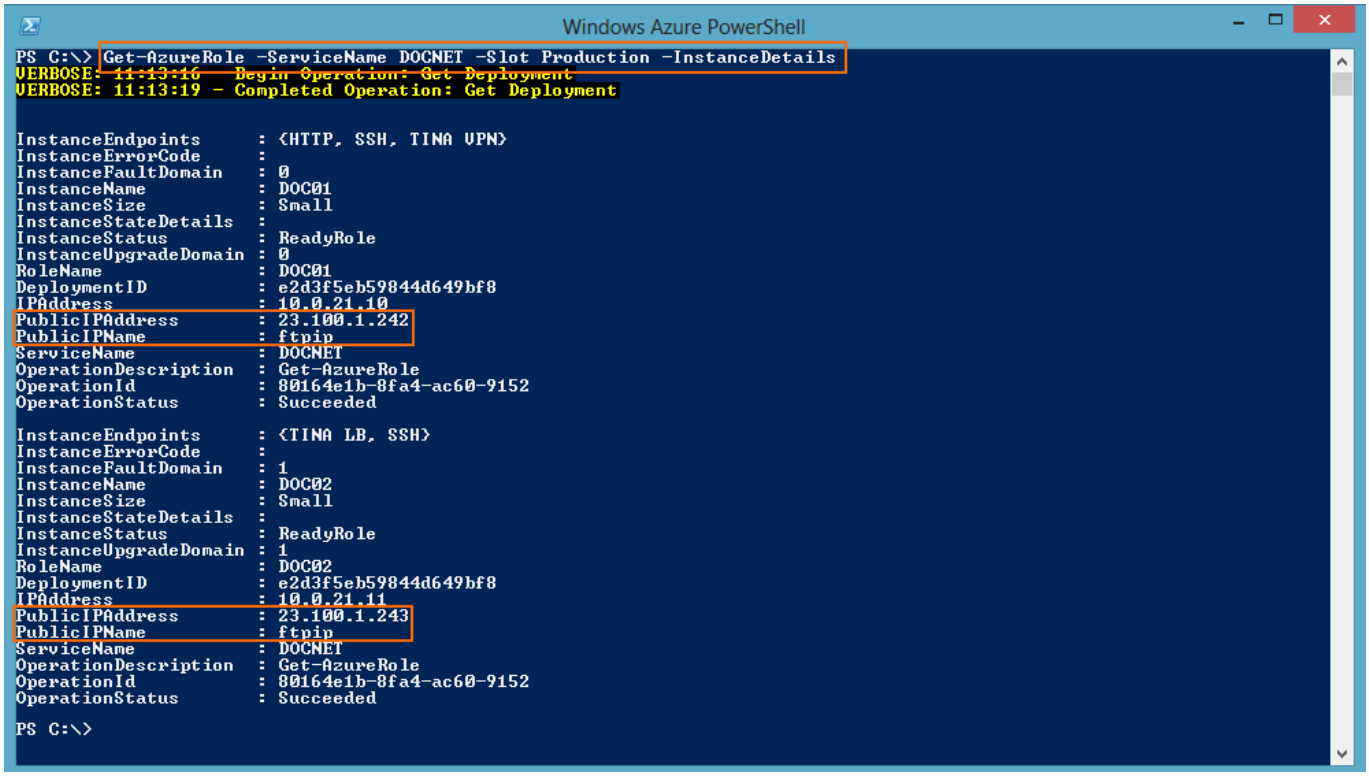
Step 4. Assign Public Instance Level IP Addresses to the Barracuda NG Firewall Virtual Machines

To access both Barracuda NG Firewall virtual machines directly, a Public Instance Level IP Address (PIP) must be assigned per VM. PIPs are managed via Azure PowerShell and are currently not visible in the Microsoft Azure web interface.

1. Launch Azure PowerShell.
2. Add a PIP to the primary Barracuda NG Firewall virtual machine:
   `Get-AzureVM -ServiceName YOUR-CLOUD-SERVICE-NAME -Name YOUR-PRIMARY-BARRACUDA-NG-FIREWALL | Set-AzurePublicIP -PublicIPName primarypip | Update-AzureVM`
3. Add a PIP to the secondary Barracuda NG Firewall virtual machine:
   `Get-AzureVM -ServiceName YOUR-CLOUD-SERVICE-NAME -Name YOUR-SECONDARY-BARRACUDA-NG-FIREWALL | Set-AzurePublicIP -PublicIPName secondarypip | Update-AzureVM`

The primary and secondary Barracuda NG Firewalls are now reachable via their own PIP. You can get PIP information on the instances by:

```
Get-AzureRole -ServiceName <your cloud="" service="" name=""> -Slot
<production or="" staging=""> -InstanceDetails</production></your>
```

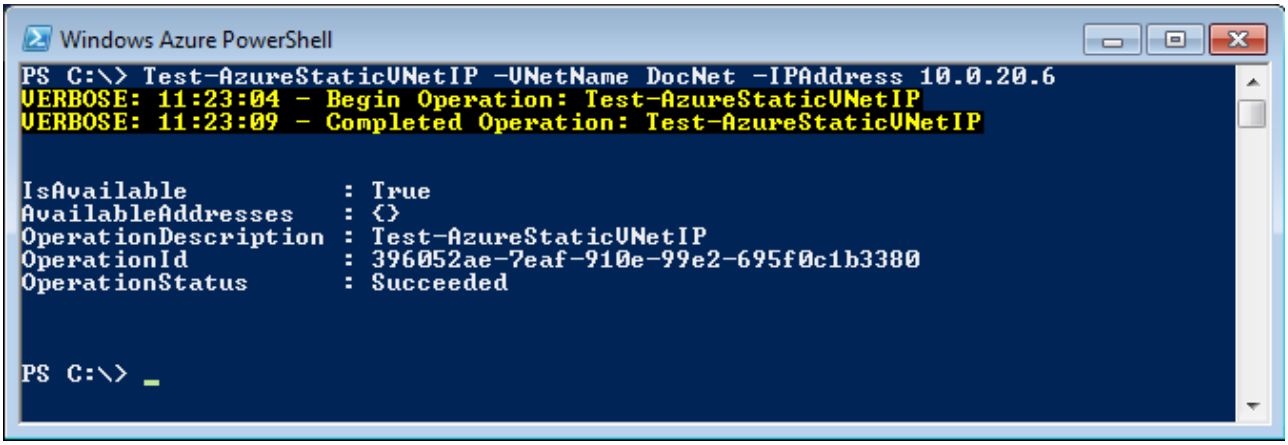


Step 5. Assign Static Internal IP Addresses to the Barracuda NG Firewall Virtual Machines

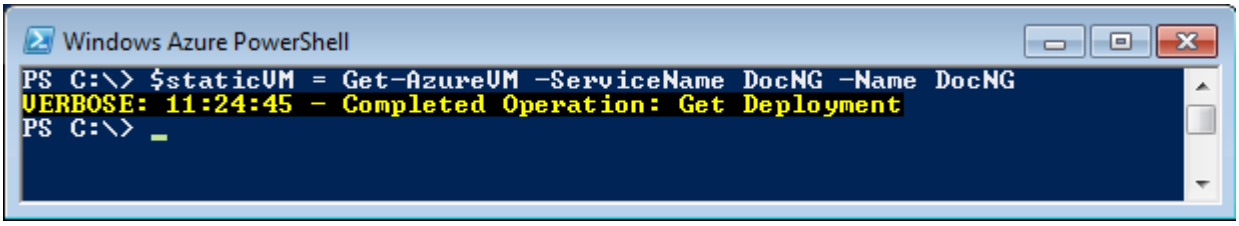
The Azure virtual machine will automatically reboot after assigning the static IP address.

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 both Barracuda NG Firewalls. They must be different from the IP addresses already assigned to the virtual machines.

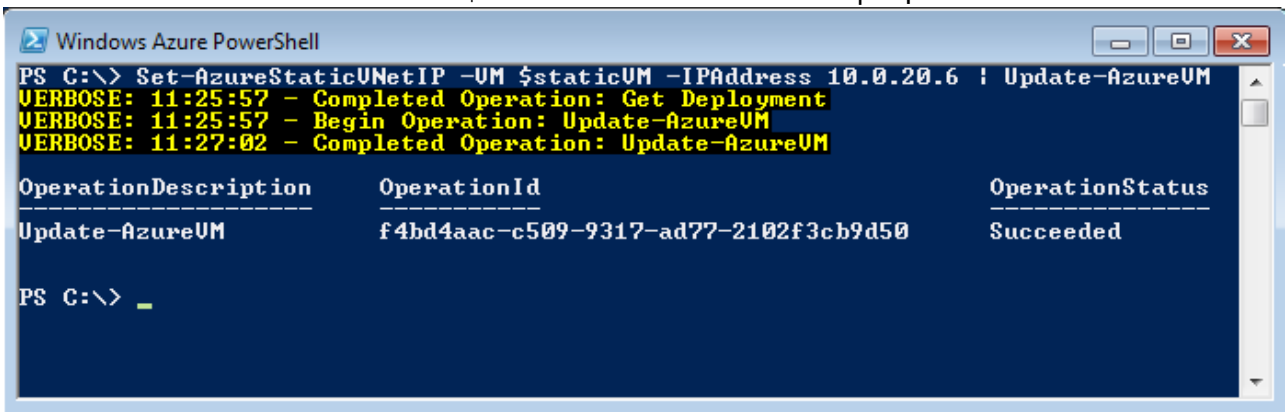
1. Open a Windows Azure PowerShell.
2. Check if the chosen IP address is available by entering:
   `Test-AzureStaticVNetIP -VNetName  -IPAddress`



3. Save the virtual machine to a local variable.
   `$staticVM = Get-AzureVM -ServiceName  -Name`

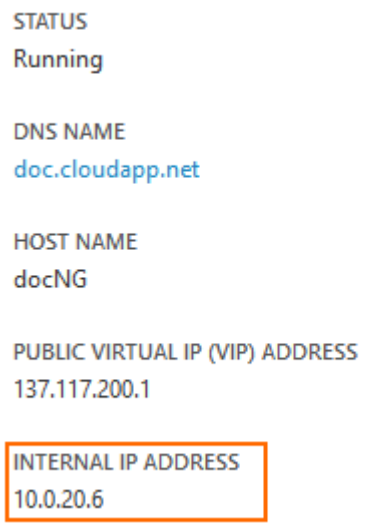


4. Change the internal IP address of the virtual machine from dynamic to static.
   `Set-AzureStaticVNetIP -VM $staticVM -IPAddress  | Update-AzureVM`



   The Barracuda NG Firewall automatically reboots.
5. Repeat the procedure for the secondary unit by using a different IP address from the same subnet.

Both Barracuda NG Firewalls are now assigned static internal IP addresses:



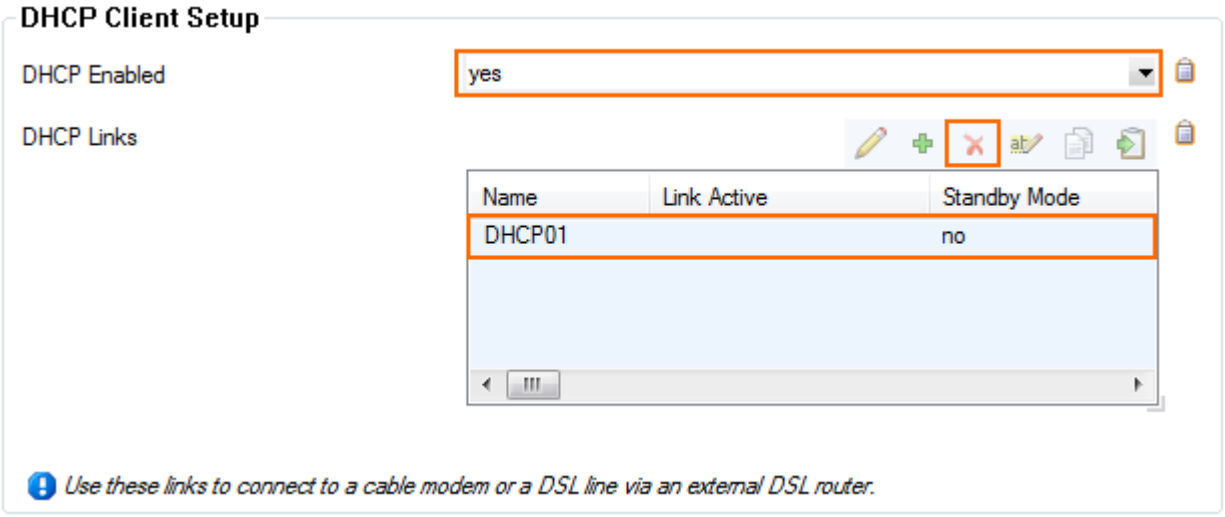
Step 6. Change the Network Configuration to Use the Static Internal IP Addresses

Change the network configuration of the primary and secondary Barracuda NG Firewall to use a static network interface.

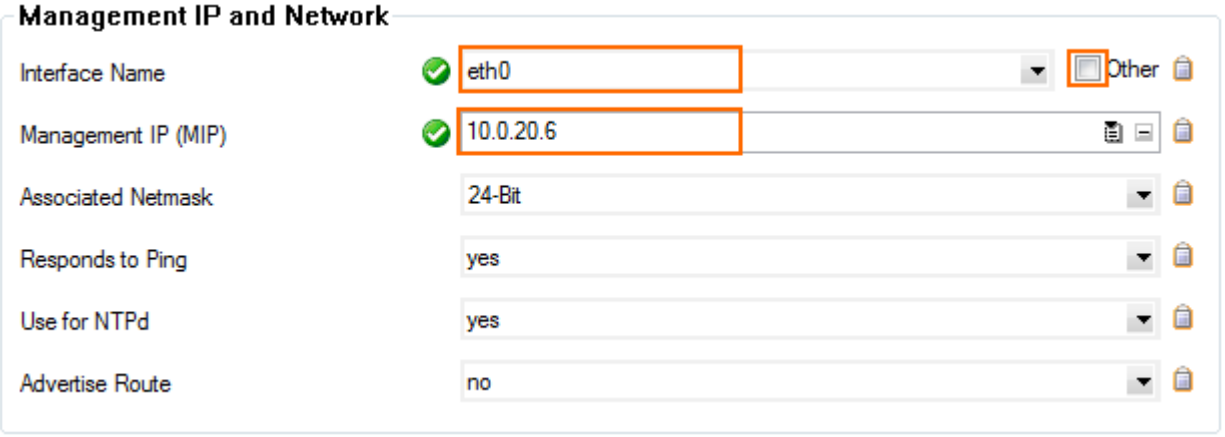
Step 6.1 Reconfigure the Network Interface

Change the network interface type from dynamic to static.

1. Log into the primary Barracuda NG Firewall via the assigned PIP.
2. Open the **Network** page (**Config > Full Config**).
3. In the left menu, click on **xDSL/DHCP/ISDN**.
4. Click **Lock**.
5. Delete the **DHCP01** entry in the **DHCP Links** list.
6. Select **No** from the **DHCP Enabled** dropdown list



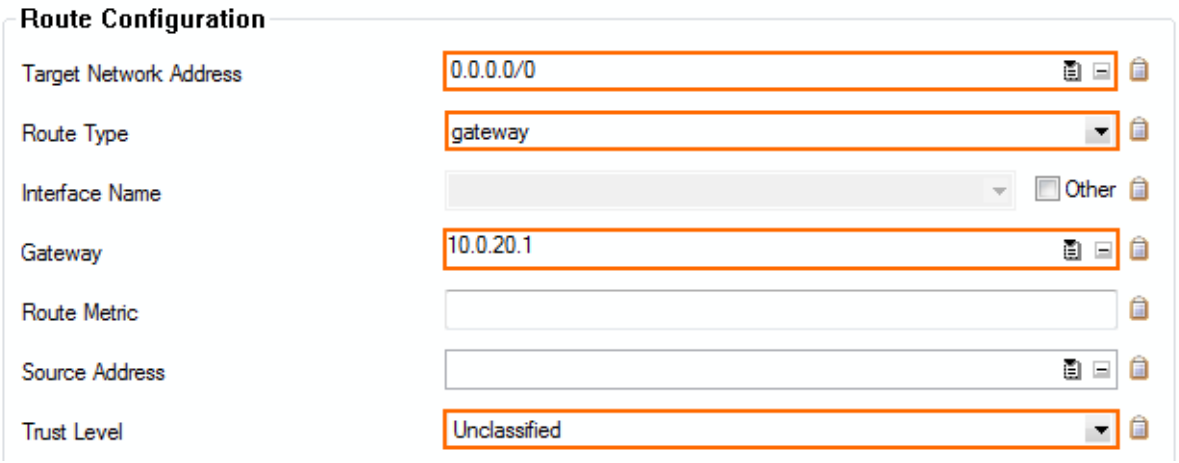
7. Click **Send Changes**.
8. In the left menu, click on **IP Configuration**.
9. In the **Management IP and Network** section in the **Interface Name** line, untick the **Other** checkbox.
10. Select **eth0** from the **Interface Name** list.
11. Enter the static internal IP address from Step 1 as the **Management IP (MIP)**. E.g., `10.0.20.6`



Step 6.3 Create the Default Route

Add the default route.

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 Barracuda NG Firewalls reside in. E.g., `10.0.20.1` if the IP addresses of the Barracuda NG Firewalls are 10.0.20.6 and 10.0.20.7
   - **Trust Level** – Select **Unclassified**.

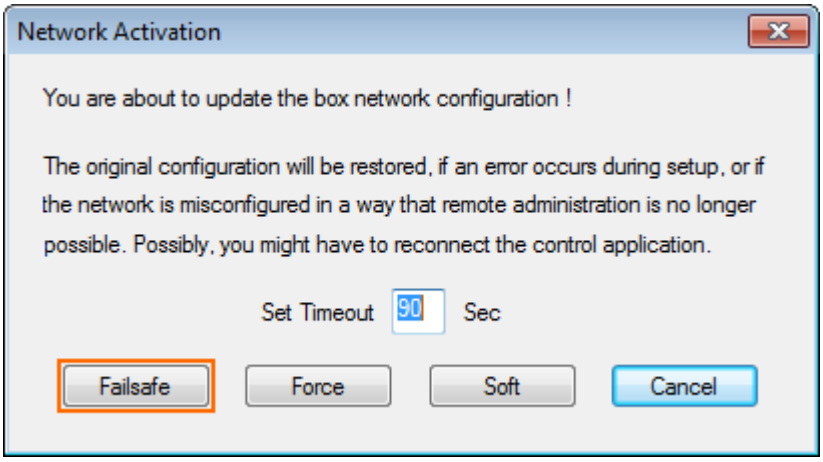


3. Click **OK**.
4. Click **Send Changes** and **Activate**.

Step 6.4 Activate the Network Changes

Activate the changes to the network configuration.

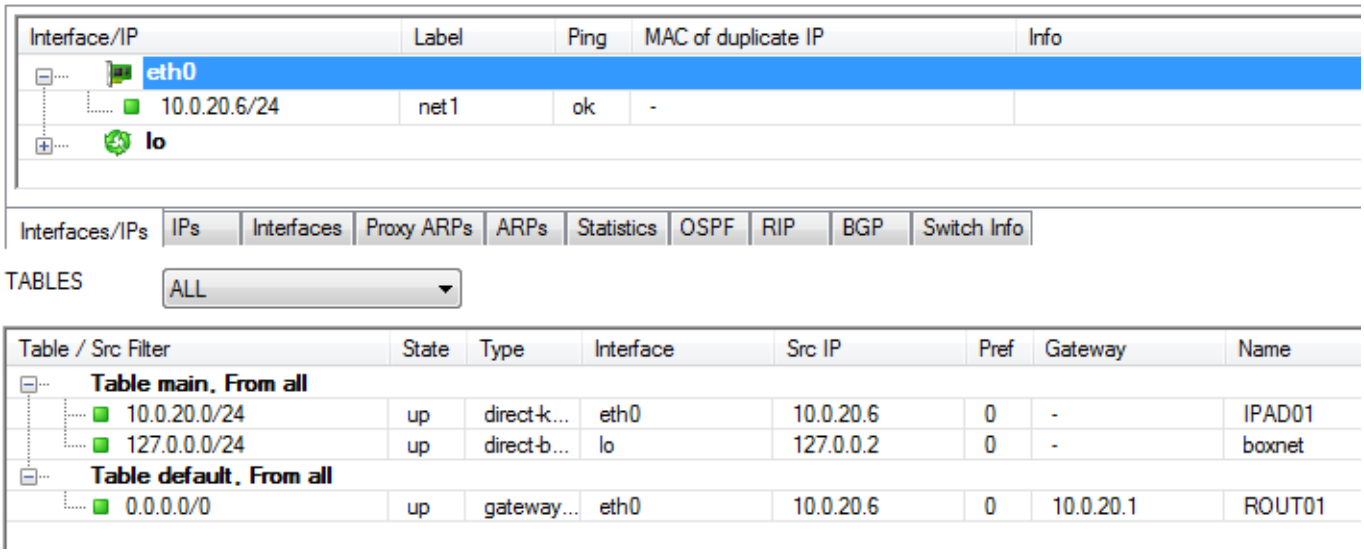
1. Open the **Box** page (**Control**).
2. in the **Network** section of the left menu, click on **Activate new network configuration**.
3. Click **Failsafe**.



Step 6.5 Reconfigure the Secondary Unit

Complete Steps 6.1 - 6.4 for the secondary unit.

Both Barracuda NG Firewall systems are now using the static 'eth0' network interfaces (**Control > Network**).



Step 7. Create a DHA Cluster Configuration

Create a DHA cluster configuration. For more information on DHA, see High Availability.

1. Log into the primary Barracuda NG Firewall.
2. Open the **Config** tab**.**
3. Right-click on **Box** and select **Create DHA Box**.
4. Open the **HA Network** page (**Config > Full Config > HA Box**).
5. Select **eth0** from the **Interface Name** list.
6. Enter the static IP address of the secondary Barracuda NG Firewall as the **Management IP (MIP)**. E.g., `10.0.20.7`
7. In the left navigation, select **Routing**.
8. Verify the default route is present. (0.0.0.0/0 gateway XX.XX.XX.1).
9. Click **Send Changes** and **Activate**.

Step 8. Deploy the HA PAR file to the Secondary Unit

Step 8.1 Create the PAR file for the HA Unit.

1. Log into the primary Barracuda NG Firewall unit.
2. Open the **Config > Full Config** page.
3. Right-click on **Box** and select **CREATE PAR FILE for HA box**. You are prompted to save the `boxha.par` file.

Step 8.2 Deploy the PAR file on the Secondary Unit

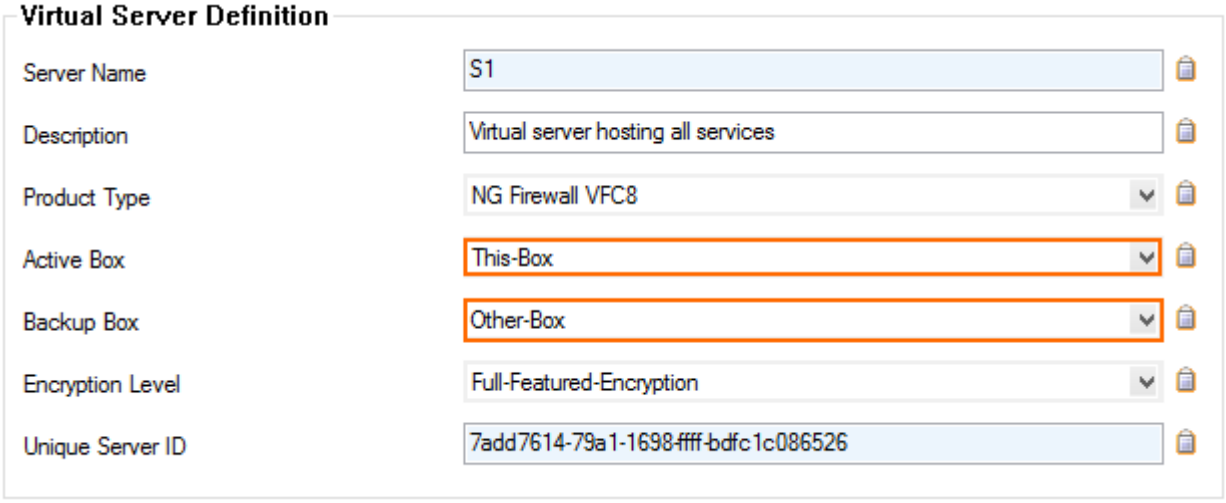
1. Log into the secondary Barracuda NG Firewall unit.
2. Open the **Config > Full Config** page.
3. Right-click on **Box** and select **Restore from PAR file**.
4. Choose the `boxha.par` file created in Step 4.1.
5. Click **Activate**.
6. Open the **Control > Box** page.
7. In the left navigation in the **Network** section, click on **Activate new network configuration**.
8. Click **Failsafe**.
9. In the left navigation in the **Operating System** section, click **Firmware Restart**.

The Barracuda NG Firewall systems are now in a high availability cluster.

Step 8.3 Set the Active and Backup Unit for the Virtual Server

Standalone NG Firewalls

1. Log into the primary unit.
2. Go to **your cluster in the NG Control Center > Virtual Servers > your virtual server > Server Properties**.
3. Click **Lock**.
4. In the **Virtual Server Definition** section, define the primary unit and secondary unit.
   - **Active Box** – Select **This-Box**.
   - **Backup Box** – Select **Other-Box**.

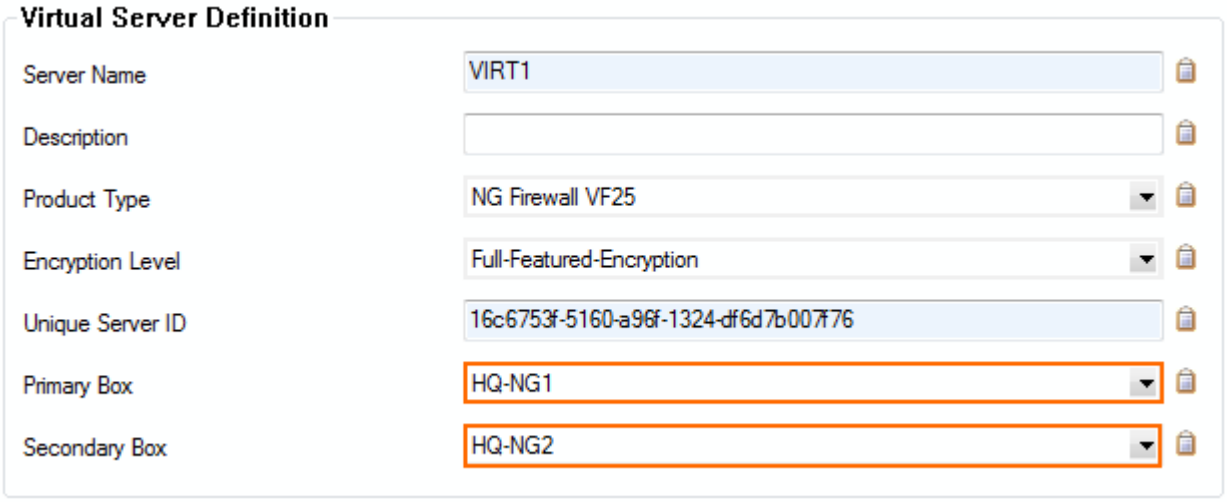


5. Click **Send Changes** and **Activate**.

Managed NG Firewalls

1. Log in to your NG Control Center.
2. Go to **your cluster in the NG Control Center > Virtual Servers > your virtual server > Server Properties**.
3. Click **Lock**.

4. In the **Virtual Server Definition** section, define the primary unit and secondary unit.
   - **Primary Box** – The active system.
   - **Secondary Box** – The HA partner.



5. Click **Send Changes** and **Activate**.

Step 9. Add Both Barracuda NG Firewall Virtual Machines to the same Availability Set

The Azure virtual machine will automatically reboot after assigning a new availability set.

To avoid hardware failures, and to take advantage of the Microsoft Azure SLA for the compute cloud, both virtual machines must be in the same availability set.

1. Log into your Microsoft Azure Management Portal (https://manage.windowsazure.com).
2. In the left pane, click on **virtual machineS.**
3. Click on the primary Barracuda NG Firewall. The **DASHBOARD** opens.
4. In the top menu, click on **CONFIGURE**.
5. Select **Create an availability set**.
6. Enter the **name** for the **AVAILABILITY SET.** E.g., HA_SET
7. In the bottom pane, click **SAVE**. Wait for the changes to be applied. The virtual machine will reboot.
8. Click on the secondary Barracuda NG Firewall. The **DASHBOARD** opens.
9. In the top menu, click on **CONFIGURE**.
10. From the **AVAILABILITY SET** list, select the availability set created for the primary Barracuda NG Firewall. E.g., **HA_SET**.
11. In the bottom pane, click **SAVE**. Wait for the changes to be applied. The virtual machine will reboot.

Both Barracuda NG Firewall systems are now in the same availability set. Go to **virtual machineS >**

> CONFIGURE . Both virtual machines are now listed below the **AVAILABILITY SET** list.

Step 10. Configure a Load Balanced Endpoint

Create a load-balanced endpoint for each Internet facing service you want to offer. E.g., a load-balanced endpoint for port UDP/691 if you are connecting via TINA to the VPN service on the HA cluster.

1. Log into your Microsoft Azure Management Portal (https://manage.windowsazure.com).
2. In the left pane, click on **VIRTUAL MACHINES**.
3. Click on the primary Barracuda NG Firewall. The **DASHBOARD** opens.
4. In the top menu, click on **ENDPOINTS**.
5. Select **ADD A STAND-ALONE ENDPOINT**.
6. Click **OK**.
7. In the **ADD ENDPOINT** window, enter:
   - **Name** – Enter a name for the endpoint.
   - **PROTOCOL** – Select **TCP** or **UDP** depending on your TINA configuration.
   - **PUBLIC PORT** – Enter the external port: E.g.,691
   - **PRIVATE PORT** – Enter the internal port. E.g., 691
   - **CREATE A LOAD-BALANCED SET** – Select the checkbox to enable load balancing for these ports.
8. Click **NEXT**.
9. Configure the load-balanced set:
   - **LOAD-BALANCED SET NAME** – Enter a name for the load balanced endpoint.
   - **PROBE PROTOCOL** – Select **TCP**.
   - **PROBE PORT** – Enter the port the service is listening on internally. E.g., 691
   - **PROBE INTERVAL** – Enter how many seconds should be between probes. Default: 5sec
   - **NUMBER OF PROBES** – Enter how many probes should be sent before the service is switched to the other unit. Default: 2
10. Click **OK**. The load-balanced endpoint is created.
11. Click on the secondary Barracuda NG Firewall. The **DASHBOARD** opens.
12. In the top menu, click on **ENDPOINTS**.
13. Select **ADD AN ENDPOINT TO AN EXISTING LOAD BALANCED SET**.
14. Select the load balanced endpoint created for the primary unit.
15. Click **NEXT**.
16. Enter a **NAME**.
17. Click **OK**.

Step 11. (optional) Remove the SETUP-MGMT-ACCESS Firewall Rule

This redirect access rule is no longer needed and can be deleted.

1. Open the **Forwarding Rules** page (**Config > Full Config > Virtual Servers > S1 > Firewall**).
2. Click **Lock**.
3. Right-click on **SETUP-MGMT-ACCESS** firewall rule and click **Delete**.
4. Click **Send Changes** and **Activate**.

You can now use the Barracuda NG Firewall HA cluster in the Microsoft Azure cloud.

Figures

1. AzureCloudHA3.png
2. vnet01.png
3. vnet02.png
4. vnet03.png
5. vnet04.png
6. cloudService01.png
7. cloudService02.png
8. cloudService03.png
9. cloudService04.png
10. PIP03.png
11. AzureHA01.png
12. AzureHA02.png
13. AzureHA03.png
14. AzureHA04.png
15. AzureHA07.png
16. AzureHA08.png
17. Azure_default_route.png
18. AzureHA10.png
19. AzureHA11.png
20. Standalone_HA_07.png
21. CC_HA_01.png