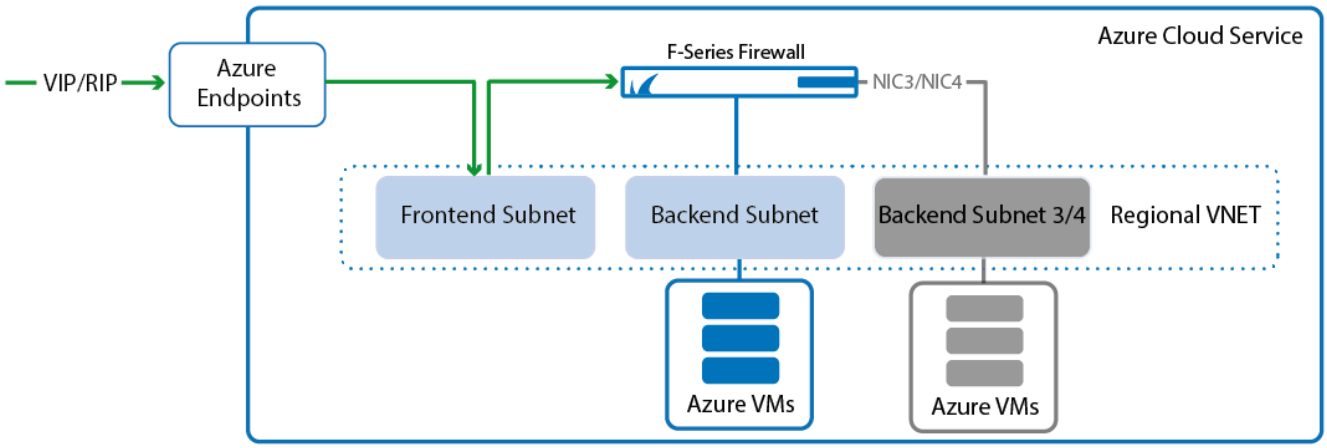
How to Deploy the Barracuda F-Series Firewall in Azure via PowerShell and ASM

https://campus.barracuda.com/doc/48202636/

For most advanced networking features in the Microsoft Azure Cloud, such as multiple network interfaces or reserved IP addresses for the Cloud Service, you must deploy the Barracuda NextGen Firewall F-Series via PowerShell. You can either enter the commands directly into the Azure PowerShell or combine the commandlets to a custom deployment script. Using a custom PowerShell script allows for rapid deployment and fast recovery in case of failure. The Barracuda NextGen Control Center for Microsoft Azure is deployed just like the NextGen Firewall F-Series except that it is limited to one network interface. The number of network interfaces depends on the Instance size:

- **Small** – One network interface
- **Medium** – One network interface
- **Large** – Up to two network interfaces
- **Extra Large** – Up to four network interfaces

Microsoft Azure charges apply. For more information, see the Microsoft Azure Pricing Calculator.



Example deployment script

You can combine the PowerShell commandlets to customize the deployment of your Barracuda NextGen Firewall F-Series in the Microsoft Azure cloud. See below for an example deployment script. This script assumes that you already configured a Regional VNET, Reserved IP (optional) in the Azure cloud, and the Azure Account for Azure PowerShell on your client.

```
#If needed import Azure PSD file
#Import-Module &amp;quot;C:\Program Files (x86)\Microsoft
```

```
SDKs\Azure\PowerShell\ServiceManagement\Azure\Azure.psd&quot;

# Use Default System Proxy
[System.Net.WebRequest]::DefaultWebProxy.Credentials =
[System.Net.CredentialCache]::DefaultCredentials

################################################
# Modify the variables below
################################################
$vmname = &quot;BNG-MultiNIC&quot;
$RootPassword = &quot;secretpa$$word&quot;
$instanceSize = &quot;Large&quot;
$cloudService = &quot;BNG-CS&quot;
$Location = &quot;North Europe&quot;
$storageAccount =&quot;mystorageaccount&quot;
#Leave empty is no reserved IP is used
$reservedIPname = &quot;&quot;
$VNetName = &quot;NG-VNET&quot;
$Subnet1 = &quot;Frontend&quot;
$Subnet2 = &quot;Backend&quot;
$NIC1IP = &quot;10.0.30.20&quot;
$NIC2IP = &quot;10.0.31.21&quot;
#Enter a VM Image name below to use a custom image. If left empty the
latest image from the Azure Marketplace is used.
$image = &quot;&quot;
$availabilitySetName =&quot;BarracudaNGAVSet&quot;
$azureSubscriptionName = &quot;Pay-As-You-Go&quot;

function AskYesNo( $title, $question, $YesInfo, $NoInfo ) {
    $yes = New-Object
System.Management.Automation.Host.ChoiceDescription
&quot;&amp;Yes&quot;, $YesInfo
    $no = New-Object System.Management.Automation.Host.ChoiceDescription
&quot;&amp;No&quot;, $NoInfo
    $options =
[System.Management.Automation.Host.ChoiceDescription[]]($yes, $no)
    $result = $host.ui.PromptForChoice($title, $question, $options, 0)
    return $result
}

Write-Host -NoNewLine &quot;This script will create a &quot;
Write-Host -NoNewLine -ForegroundColor yellow &quot;dual-NIC Barracuda
NextGen Firewall F-Series&quot;
Write-Host &quot; instance in Azure&quot;
Write-Host &quot;&quot;
Write-Host -NoNewLine &quot;Vnet name: &quot;
```

```
Write-Host -ForegroundColor yellow $VNetName
Write-Host -NoNewLine &quot;NIC 1: &quot;
Write-Host -NoNewLine -ForegroundColor yellow &quot;$NIC1IP in
$Subnet1&quot;
Write-Host &quot; (management)&quot;
Write-Host -NoNewLine &quot;NIC 2: &quot;
Write-Host -ForegroundColor yellow &quot;$NIC2IP in $Subnet2&quot;
Write-Host -NoNewLine &quot;Azure DC: &quot;
Write-Host -ForegroundColor yellow $Location

if ($reservedIPName -ne &quot;&quot;)
{
    Write-Host &quot;Using the Existing Reserved IP address:
$reservedIPName&quot;
}

$yesorno = AskYesNo 'Do you want to continue?' $warn 'aborting script'
'using existing VNET'
    switch ( $yesorno ) {
        0 { &quot;OK! Creating a new Barracuda NextGen Firewall F-Series
VM.&quot; }
        1 {
            &quot;Got it :( Please correct variable values in script and
rerun.&quot;
            return
        }
    }

# Create storage if it doesn't exist yet
if(!(Test-AzureName -Storage $storageAccount))
{
    Write-Host &quot;Creating Storage Account $storageAccount in
$Location&quot;
    New-AzureStorageAccount -StorageAccountName $storageAccount -
Location $Location
}

if ($reservedIPName -ne &quot;&quot;)
{
$reservedIP = Get-AzureReservedIP -ReservedIPName $reservedIPName
Write-Host &quot;Using Existing Reserved IP!&quot;
}

# Set storage account as default storage
Set-AzureSubscription -SubscriptionName $azureSubscriptionName -
CurrentStorageAccountName $storageAccount
```

```
# If no explicit image is defined get the latest Barracuda NextGen
Firewall F-Series Azure Image available in the Azure Marketplace
if ( $image -eq &quot;&quot;)
{
    $image = Get-AzureVMImage | where { $_.ImageFamily -Match
&quot;Barracuda NextGen Firewall*&quot;} | sort PublishedDate -
Descending | select -ExpandProperty ImageName -First 1
    Write-Host &quot;Using Image from Azure Marketplace...&quot;
}

# Create Azure VM
$vm1 = New-AzureVMConfig -Name $vmname -InstanceSize $instanceSize -
Image $image &ndash;AvailabilitySetName $availabilitySetName
Add-AzureProvisioningConfig -Linux -LinuxUser &quot;azureuser&quot; -
Password $RootPassword -VM $vm1 -NoSSHEndpoint

# Add Endpoints for 1st NIC of the Barracuda NextGen Firewall F-Series
Add-AzureEndpoint -Protocol tcp -LocalPort 22 -PublicPort 22 -Name
&quot;SSH&quot; -VM $vm1
Add-AzureEndpoint -Protocol tcp -LocalPort 807 -PublicPort 807 -Name
&quot;MGMT&quot; -VM $vm1
Add-AzureEndpoint -Protocol tcp -LocalPort 691 -PublicPort 691 -Name
&quot;TINATCP&quot; -VM $vm1
Add-AzureEndpoint -Protocol udp -LocalPort 691 -PublicPort 691 -Name
&quot;TINAUDP&quot; -VM $vm1
Write-Host &quot;Added Endpoints...&quot;

# Define Subnet and static IP Address for 1st NIC
Set-AzureSubnet -SubnetName $Subnet1 -VM $vm1
Set-AzureStaticVNetIP -IPAddress $NIC1IP -VM $vm1
Write-Host &quot;Configured First NIC...&quot;

# Add Additional NICS
Add-AzureNetworkInterfaceConfig -Name &quot;NIC2&quot; -SubnetName
$Subnet2 -StaticVNetIPAddress $NIC2IP -VM $vm1
Write-Host &quot;Added Second NIC...&quot;

# Create Barracuda NextGen Firewall F-Series VM
if ($reservedIPName -eq &quot;&quot;)
{
    New-AzureVM -ServiceName $cloudService -VM $vm1 -Location $Location
-VNetName $VNetName
    Write-Host &quot;Creating VM without Reserved IP Address...&quot;
}
else
{
```

```
    New-AzureVM -ServiceName $cloudService -VM $vm1 -ReservedIPName
$reservedIPName -Location $Location -VNetName $VNetName
    Write-Host &quot;Creating VM with Reserved IP Address
$reservedIPName... &quot;
}
Write-Host &quot;Script is done. Creating the Virtual Machine can take a
while. Have a cup of coffee! Use NextGen Admin to login to
$cloudService.cloudapp.net: user: root, password: $RootPassword)&quot;
```

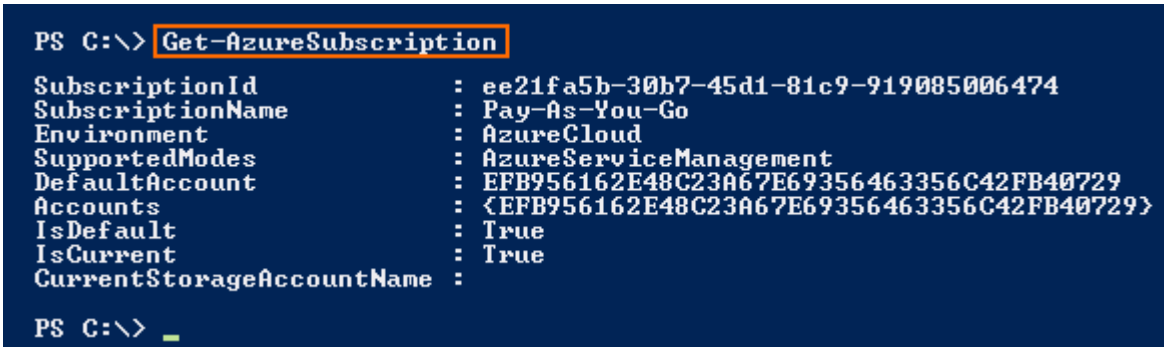
Before you begin

- Create a Microsoft Azure account.
- Download and install Azure PowerShell. 0.9.8.
  > Azure PowerShell 1.0.1 introduces changes not compatible with the instructions in this article.
- Purchase a Barracuda NextGen Firewall F-Series Azure license or get a license from the Barracuda Networks Evaluation page:
  1. From the **Select a Product** list, select **Barracuda NextGen Firewall F-Series Azure** under the **Public Cloud Solutions** category.
  2. From the **Select Edition** list, select the Level that you want. Azure Level 3 or 4 required for multi-NIC Deployments
  3. Complete and submit the rest of the form. You will receive an email containing your serial number and license token.

Step 1. Configure your Azure PowerShell to use your Azure account

Import the Azure Subscription file, to associate Azure PowerShell with your Azure account.

1. Open an Azure PowerShell.
2. To download your publishsettingsfile, enter:
   `Get-AzurePublishSettingsFile`
3. The download popup of your browser opens. Save the file.
4. Import the publishsettingsfile by entering:
   `Import-AzurePublishSettingsFile PATH_TO_FILE`
5. Check your subscription by entering. If **CurrentStorageAccountName** is set, make sure that the storage account is in the same location you want to create the VM in.
   `Get-AzureSubscription`



Step 2. Create an Azure regional virtual network

You must use a Regional VNet to deploy the Barracuda NextGen Firewall F-Series. Older Affinitygroup-based VNets are not compatible with reserved static IP addresses, static internal IP addresses, Public IP Addresses (PIP), or multiple network interfaces. Configuration information of the VNet is stored in an XML file and then deployed in the Azure Cloud via PowerShell commandlet. An example vmnet.xml with 2 subnet:

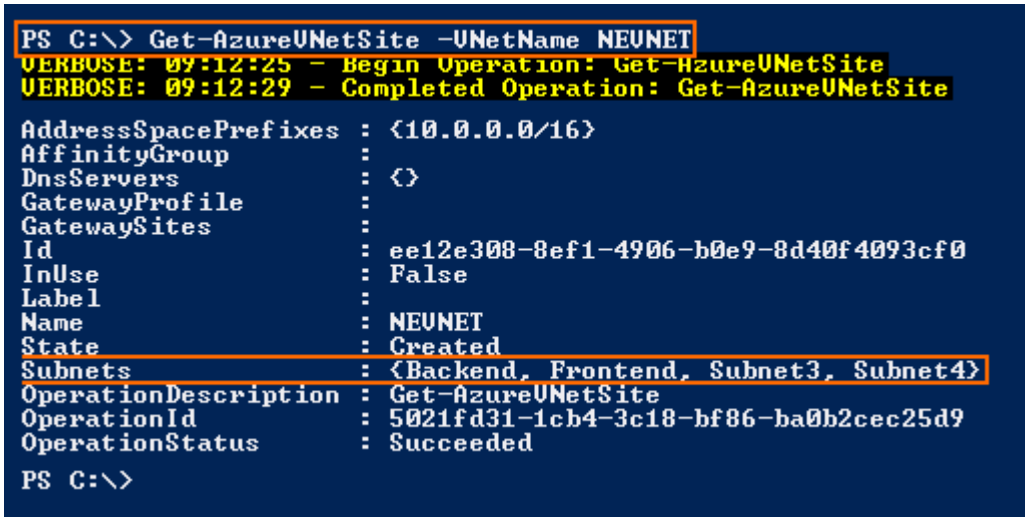
```
&lt;NetworkConfiguration
xmlns=&quot;http://schemas.microsoft.com/ServiceHosting/2011/07/NetworkC
onfiguration&quot;&gt;
  &lt;VirtualNetworkConfiguration&gt;
   &lt;VirtualNetworkSites&gt;
      &lt;VirtualNetworkSite name=&quot;NEVNET&quot;
Location=&quot;North Europe&quot;&gt;
        &lt;AddressSpace&gt;
          &lt;AddressPrefix&gt;10.0.0.0/16&lt;/AddressPrefix&gt;
        &lt;/AddressSpace&gt;
        &lt;Subnets&gt;
          &lt;Subnet name=&quot;Frontend&quot;&gt;
            &lt;AddressPrefix&gt;10.0.30.0/24&lt;/AddressPrefix&gt;
          &lt;/Subnet&gt;
              &lt;Subnets&gt;
          &lt;Subnet name=&quot;Backend&quot;&gt;
            &lt;AddressPrefix&gt;10.0.31.0/24&lt;/AddressPrefix&gt;
          &lt;/Subnet&gt;
                &lt;/Subnets&gt;
           &lt;/VirtualNetworkSite&gt;
    &lt;/VirtualNetworkSites&gt;
  &lt;/VirtualNetworkConfiguration&gt;
&lt;/NetworkConfiguration&gt;
```

1. Open the Azure PowerShell.

2. If VNets already exist, export the existing Virtual Networks to a xml file
   `Get-AzureVNetConfig -ExportToFile c:\azure\vmnet.xml`
3. Edit the vnet.xml file and enter the configuration for your **VIRTUALNETWORKSITE.** Use the example file above as a guideline. If you are using multiple network interfaces, create one subnet per network interface.
4. Upload the VNet configuration file:
   `Set-AzureVNetConfig -ConfigurationPath PATH-TO-YOUR-VNET-XML-FILE`

The virtual network is now listed in **VIRTUAL NETWORKS** in the web UI, via PowerShell:

```
Get-AzureVNetSite -VNetName "YOUR VNET NAME"
```



Step 3. (optional) Use a reserved IP for the Azure Cloud service

To avoid the difficulty of changing IP address when redeploying your Cloud Service, you can reserve a public IP address and assign it when creating a cloud service. This IP address persists even when the cloud service that it is assigned to is deleted.

Create a Reserved IP address (RIP).

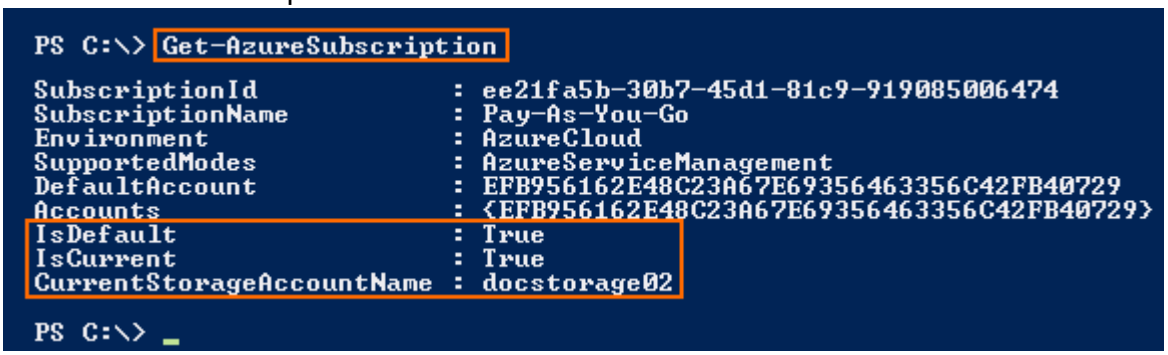
```
New-AzureReservedIP -ReservedIPName "RIP NAME" -Label "NextGen Firewall F-Series IP" -Location "YOUR LOCATION"
```

Step 4. Create a storage account

1. Create a Storage Account and set it as the default storage account.
   `New-AzureStorageAccount -StorageAccountName "STORAGEACCOUNT NAME" -`

```
Location "YOUR LOCATION"
```

2. Use the storage account as the default storage account for this Azure subscription.
   ```
   Set-AzureSubscription -SubscriptionName "YOUR AZURE SUBSCRIPTION NAME" -CurrentStorageAccountName "STORAGEACCOUNT NAME"
   ```
3. Verify that you are using the correct storage account:
   ```
   Get-AzureSubscription
   ```



Step 5. Get a NextGen Firewall F-Series image

You can either create your own image from a VHD file you have uploaded to the storage account, or use the Barracuda NextGen Firewall F-Series image from the Azure Marketplace.

Get the ID of the Firewall image from the Azure Marketplace (recommended)

To deploy the VM image of the Barracuda NextGen Firewall F-Series from the Azure Gallery, you need to find the exact image name. E.g., for 5.4.3 the image name is: **810d5f35ce8748c686feabed1344911c__BarracudaNGFirewall-5.4.3-182-pl4**. The Azure image name changes every time the image in the Azure Gallery is updated.

1. Open an Azure PowerShell.
2. Get a list of all available Azure images in the Azure Gallery and only show the ones for the Barracuda NextGen Firewall F-Series and store the image name in a variable. E.g., $image
   ```
   $image = Get-AzureVMImage | where { $_.ImageFamily -Match "Barracuda NextGen Firewall F-Series*"} | sort PublishedDate -Descending | select -ExpandProperty ImageName -First 1
   ```

Upload a VHD disk image and create the virtual machine (alternative)

If you want to deploy a version of the Barracuda NextGen Firewall F-Series that is not available in the Azure Marketplace, or want to be certain to always deploy the exact same firmware version of the Barracuda NextGen Firewall F-Series, upload a VHD disk image and create your own Virtual Machine.

1. Download the VHD file from https://login.barracudanetworks.com.
2. Create a new Azure Storage Container.

New-AzureStorageContainer -Name <name of storage container>
`New-AzureStorageContainer -Name "images"`

3. Upload the VHD to the Azure storage account.
   Add-AzureVhd -Destination <storage account URL>/<storage container name>/filename.vhd -LocalFilePath -NumberOfUploaderThreads 4
   `Add-AzureVhd -Destination https://docstorage02.blob.core.windows.net/images/GWAY-6.0.0-190.vhd -LocalFilePath c:\Azure\GWAY-6.0.0-190.vhd -NumberOfUploaderThreads 4`
   Depending on your connection, uploading the disk image might take a long time.
4. Create a Virtual Machine from the VHD disk image and save the Virtual Machine in a variable so it can be used as a parameter later:
   `$vmimage = Add-AzureVMImage -ImageName IMAGE_NAME -MediaLocation STORAGE_ACCOUNT_URL/CONTAINER/VHD_DISK_IMAGE_FILE.vhd -Label YOUR_LABEL -OS "Linux" $image = $vmimage.ImageName`

Step 6. Create and provision the Azure configuration for the new Firewall F-Series virtual machine

Create the configuration for the new Azure Virtual Machine by defining VM size, the VM image created in step 4, and the Availability Set. If you want to use multiple Network interfaces, you must use a **Large** or **Extra Large** Instance. **Large** Instances support two Network Interfaces, **Extra Large** Instances four Network Interfaces. The **LinuxUser** parameter is ignored, and the password set is used for the root user on the Barracuda NextGen Firewall F-Series.

```
$vm1 = New-AzureVMConfig -Name "VMNAME" -InstanceSize $instanceSize -Image $image -AvailabilitySetName "NGHACluster" Add-AzureProvisioningConfig -Linux -LinuxUser "azureuser" -Password "SUPERSECRETPASSWORD" -VM $vm1 -NoSSHEndpoint
```

Step 7. (optional) Add endpoints

Add Endpoints for SSH, Barracuda NextGen Admin, and all services (e.g., VPN, SSL VPN,..) running on the Barracuda NextGen Firewall F-Series. You can also add Endpoints later.

```
Add-AzureEndpoint -Protocol tcp -LocalPort 22 -PublicPort 22 -Name "SSH" -VM $vm1 Add-AzureEndpoint -Protocol tcp -LocalPort 807 -PublicPort 807 -Name "MGMT" -VM $vm1 Add-AzureEndpoint -Protocol tcp -LocalPort 691 -PublicPort 691 -Name "TINAVPN" -VM $vm1
```

Step 8. Assign the subnet and a static IP address to the first network interface

You need to assign the subnet in the VNET to the first Network Interface of the Azure Instance. Note that you can define Endpoints only for the first Network Interface of a VM.

1. Before you assign a static IP address to the VM, check to see if the IP address is available or already in use by another VM
   `Test-AzureStaticVNetIP -VNetName "VNET NAME" -IPAddress "FRONTEND STATIC IP"`
2. Assign the subnet and
   `Set-AzureSubnet -SubnetName "FRONTEND SUBNET NAME" -VM $vm1 Set-AzureStaticVNetIP -IPAddress "FRONTEND STATIC IP" -VM $vm1`

Step 9. (optional) Add additional network interfaces

Depending on the Azure Instance size, add one or two additional Network Interfaces to your VM. Each Network Interface is assigned a static IP address in their Subnet. You can only use one Network Interface per Subnet.

Limitations of multiple network interfaces

- Multiple NIC is supported on Large and Extra Large Azure VMs. VMs must be in a location-based Azure Virtual Network.
- Adding or removing NICs after a VM is created is not possible.
- NICs in Azure VMs cannot act as Layer 3 gateways.
- Internet-facing VIP RIP is only supported on the first default NIC, and there is only one VIP mapped to the IP of the default NIC. The additional NICs cannot be used in a Load Balance set.
- The order of the NICs inside the VM will be random, but the IP addresses and the corresponding MACs will remain the same.
- You cannot apply Network Security Groups or Forced Tunneling to the non-default NICs.

1. Check if the desired IP address is available:
   `Test-AzureStaticVNET -VNetName "VNET NAME" -IPAddress "BACKEND STATIC IP"`
2. Add a second Network Interface:
   `Add-AzureNetworkInterfaceConfig -Name "NIC2" -SubnetName "BACKEND SUBNET NAME" -StaticVNetIPAddress "BACKEND STATIC IP" -VM $vm1`
3. If you are using an Extra Large Instance, you can add two additional Network Interfaces (four

total).

Step 10. Create the Barracuda NextGen Firewall F-Series virtual machine

You can now create the Barracuda NextGen Firewall F-Series virtual machine.

With a reserved IP address:

```
New-AzureVM -ServiceName "CLOUD SERVICE NAME" -VM $vm1 -ReservedIPName
"RESERVED IP NAME" -Location "YOUR LOCATION" -VNetName "VNET NAME"
```

Without a reserved IP address:

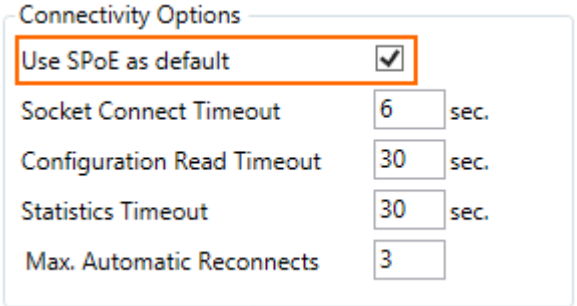
```
New-AzureVM -ServiceName "CLOUD SERVICE NAME" -VM $vm1 -Location "North
Europe" -VNetName "VNET NAME"
```

Step 11. Configure NextGen Admin

You must use the latest version of **Barracuda NextGen Admin** to connect to your Barracuda NextGen Firewall F-Series Azure.

You must use Single Point of Entry (SPoE) to connect to the Barracuda NextGen Firewall F-Series in the Azure cloud. SPoE is enabled per default.

1. Launch NextGen Admin.
2. In the upper left-hand corner, click **Option** and **Settings**.
3. Select the check box for **SPoE as default**.



Next steps

- You can now connect to your Barracuda NextGen Firewall F-Series in the Microsoft Azure cloud.
- Activate the license on both firewalls. For more information, see How to Activate and License a Stand-alone Virtual or Public Cloud F-Series Firewall or Control Center.
- Configure the additional network interfaces on the Barracuda NextGen Firewall F-Series by using Barracuda NextGen Admin. For more information, see How to Add Additional Network Interfaces.
- Configure direct attached routes for the additional network interfaces. For more information, see How to Configure Direct Attached Routes.
- Add one IP address per subnet to the virtual server IP addresses. For more information, see Virtual Servers and Services.
- To use two firewalls in a high availability (HA) cluster, see High Availability in Azure.

Figures

1. azure_deployment_mn.png
2. AzureMN_00.png
3. AzureMN_01.png
4. AzureMN_02.png
5. SPOE.png