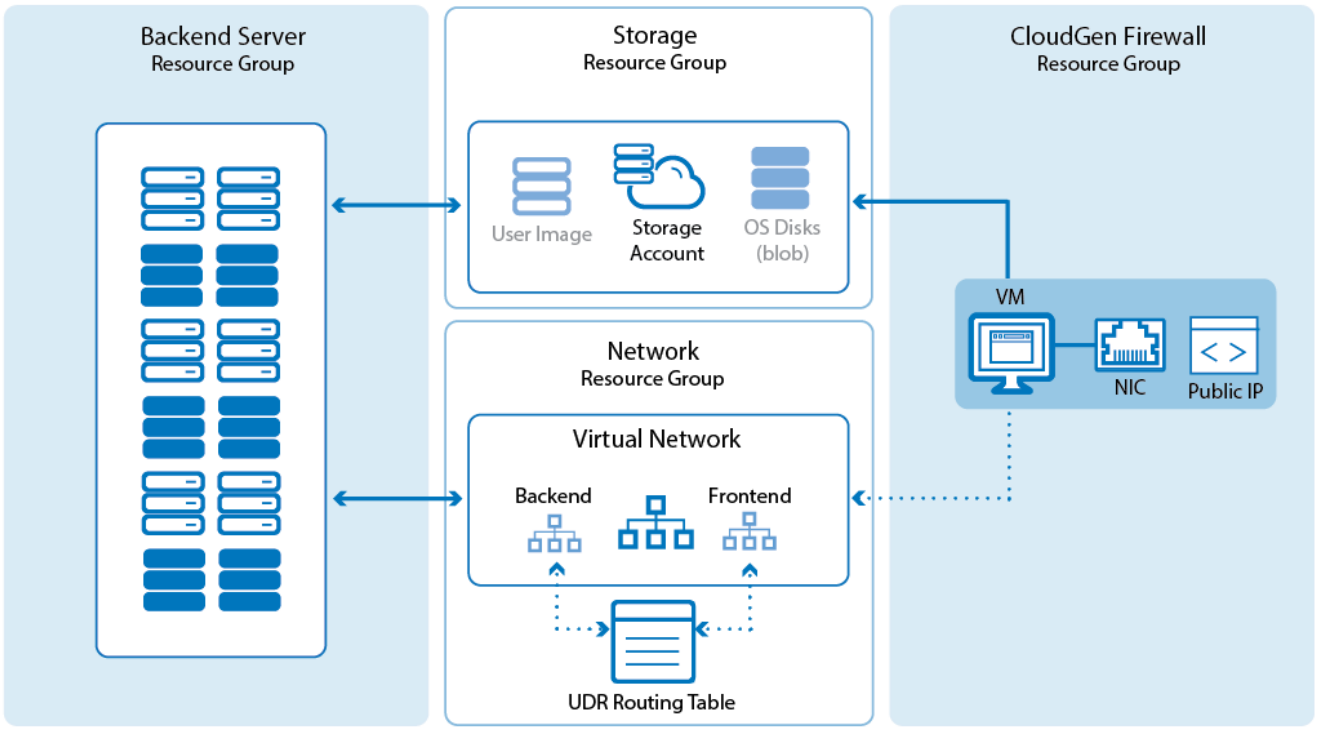
How to Deploy a CloudGen Firewall in Microsoft Azure Using PowerShell and ARM

https://campus.barracuda.com/doc/79463340/

For most advanced networking features in the Microsoft Azure Cloud, such as multiple network interfaces or user images, deploy the CloudGen Firewall F via PowerShell script. The script used in this article is hosted on the Barracuda Networks GitHub account in the **ngf-automation** repository.

Using a custom PowerShell script allows for rapid deployment and fast recovery in case of failure. The Firewall Control Center for Microsoft Azure is deployed just like the firewall except that it is limited to one network interface. The maximum number of network interfaces depends on the instance size. To organize the resources in the cloud, it is recommend to use multiple resource groups. This makes it possible to separate storage from networking and the VMs. You can also assign different permissions in Azure to control access to the resources. It is recommended to use at least two resource groups:

- **Networking resource group** – Contains the Azure Virtual network. For high availability (HA) clusters, the load balancer would also be placed in this resource group. You can also add VNET to VNET Azure VPN Gateways to this group. For stand-alone NGF VMs, you can also add the UDR route table to this resource group.
- **CloudGen Firewall F resource group** – Contains the firewall VM as well as NICs, public IP addresses, and, if needed, the UDR routing table for HA clusters.
- **(optional) Storage resource group** – Contains the storage accounts holding user-defined images and OS disk images for the VMs. This is not needed if managed disks are used.



Before You Begin

- Download the latest version of the **ngf_deploy.ps1** script from the Barracuda Networks GitHub account.
- Install Azure PowerShell version 4.3.1 or higher.
- (BYOL license only) Purchase a Barracuda CloudGen Firewall F or Control Center for Azure license, or request an evaluation license from the Barracuda Networks Evaluation page.

Step 1. Edit the Parameters in the PowerShell Script

1. Edit the **ngf_deploy.ps1** script.
2. Enter the Azure datacenter location:
   - **$location** – Enter the Azure location. E.g., 'West Europe'.
3. Enter disk and, optionally, the storage account settings:
   - **$useManagedDisks** – Set to **$true** to use managed disks. It is recommended to use managed disks.
   - **$storageAccountName** – Enter your storage account name if you are not using managed disks.
   - **$storageAccountContainerName** – Enter your BLOB container name if you are not using managed disks.
   - **$storageAccountResourceGroupName** – Enter the storage resource group name if you are not using managed disks.
   - **$datadisksize** – Enter the size of each data disk. Data disks are added as a RAID5. E.g., = 3 X 40GB in RAID5 = 80 GB of usable capacity.
   - **$storageType** – Enter the storage type used for the firewall VM: **'StandardLRS'** for magnetic or **'PremiumLRS'** for SSD storage. The VM size used for the firewall must support this storage type.
4. Configure which image is deployed:
   - **$customSourceImageUri** – Leave empty to use the latest image from the Azure Marketplace. To use a user defined image, enter the image URL. E.g., https://docstorage0.blob.core.windows.net/vhds/GWAY-6.2.0-216-Azure.vhd
   - **$vmLicenseType** – Enter **'hourly'** to use the PAYG image, or **'byol'** for the BYOL image from the Azure marketplace. This value is ignored if a user defined image is used.
   - **$vmProductType** – Enter '**barracuda-ng-firewall**' to deploy a CloudGen Firewall or **'barracuda-ng-cc'** to deploy a Firewall Control Center. This value is ignored if a user defined image is used.
5. Configure the VNET settings:
   - **$vnetName** – Enter your VNET name.
   - **$vnetResourceGroupName** – Enter the resource group of your VNET.
6. Enter the name of the availability set:
   - **$vmAvSetName** – Enter the name for the availability set. It is recommended to always use an availability set in case you want to deploy a second firewall for high availability

later.

7. Enter the private static IP address to be used by the firewall VM:
   - **$nic1InternalIP** – Enter an unused IP address in the firewall subnet. The first four and the last IP address in the subnet are always reserved by Azure. Leave empty to dynamically assign an IP address in the subnet.
8. Configure the desired VM name and resource group:
   - **$NGFResourceGroupName** – Enter the name of the resource group that is created for the firewall VM.
   - **$rootPassword** – Enter the password set for the root user during provisioning.
   - **$vmSuffix** – Enter a string such as **'NGF'**. This string is prepended to the resources created for the firewall VM and also used as the VM name.
   - **$vmSize** – Enter the VM size matching the used storage type. E.g., 'Standard_A3'
9. Save the script.

Step 2. Run the PowerShell Script

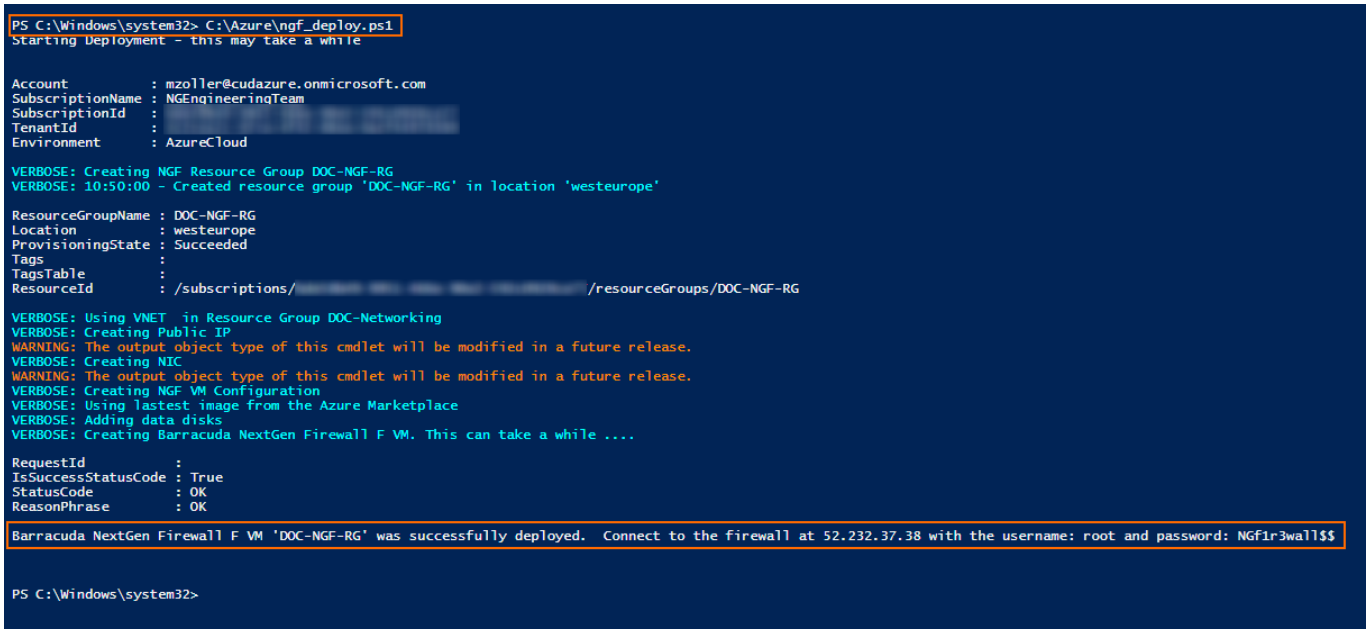
1. Open a PowerShell terminal.
2. Execute the **ngf_deploy.ps1** script.

```
\PATH_TO_SCRIPT\ngf_deploy.ps1
```

3. Enter your Azure credentials when prompted.

   Wait for the firewall VM to be created. This may take a couple of minutes depending on the VM size.

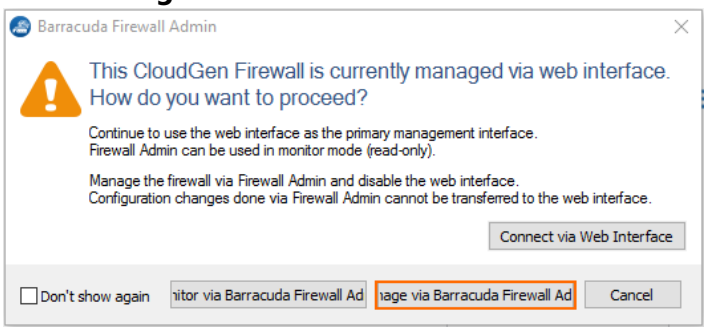
The public IP address, username, and password for the deployed CloudGen Firewall is displayed after a successful deployment.



Step 3. Log In via Barracuda Firewall Admin

Verify that Barracuda Firewall Admin is configured to use SPoE as the connection method.

1. Launch Barracuda Firewall Admin.
2. Verify that SPoE is enabled in the Barracuda Firewall Admin settings. For more information, see Barracuda Firewall Admin Settings.
3. Select **Firewall**.
4. Enter the login information:
   - **Management IP** – Enter the public IP address of your firewall VM from Step 5.
   - **Username** – Enter `root`.
   - **Password** – Enter the password you set during deployment.
5. Click **Sign In**.
6. Renew your password.
7. The window for selecting how to manage the firewall is displayed.
8. Click **Manage via Barracuda Firewall Admin**.



You are now successfully logged into your CloudGen Firewall F VM.

Next Steps

- Activate the license. For more information, see How to Activate and License a Stand-alone Virtual or Public Cloud Firewall or Control Center.
- (**Important!**) Limit access to the management ports of the Barracuda CloudGen Firewall (TCP/807 and TCP/22) to only specific source IP addresses. For more information, see How to Change the Root Password and Management ACL.
- Configure UDR Azure route table. For more information, see How to Configure Azure Route Tables (UDR) using PowerShell and ARM.
- Configure Azure cloud integration on the firewall. For more information, see How to Configure Azure Cloud Integration using ARM.
- To use two firewalls in an HA cluster, see How to Configure a High Availability Cluster in Azure using PowerShell and ARM.

Figures