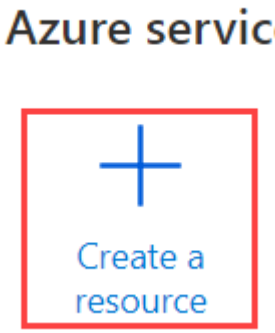
Deploying and Provisioning the Barracuda Web Application Firewall in the New Microsoft Azure Management Portal

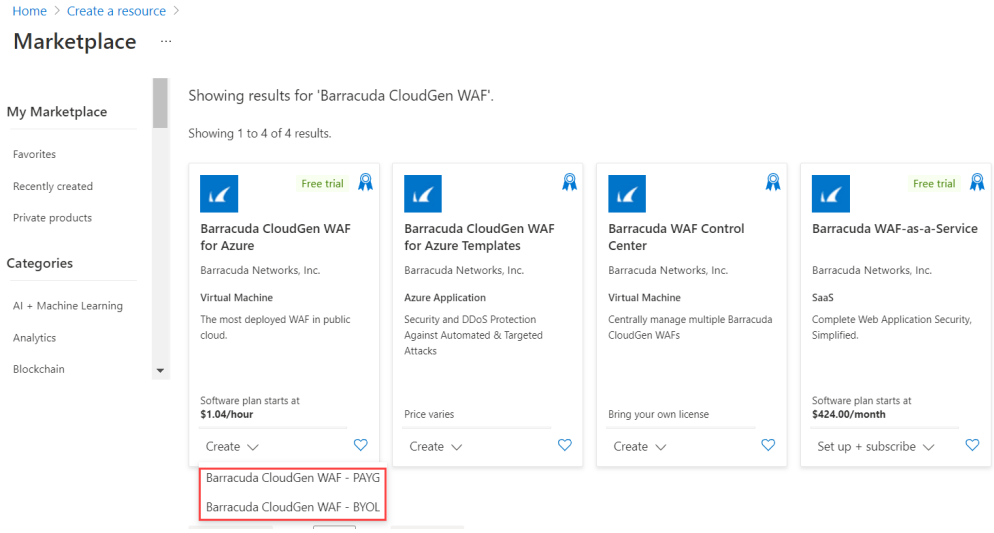
https://campus.barracuda.com/doc/49056904/

Perform the following steps to deploy and provision the Barracuda Web Application Firewall using Resource Manager in the new Microsoft Azure portal:

1. Log into the Microsoft Azure Management Portal.
2. Click **Create a resource** under Azure services.



3. In the **Search services and marketplace** text field, enter `Barracuda Web Application Firewall for Azure` and click **Enter**.
4. In the search results, click the **Create** drop-down list under **Barracuda Web Application Firewall for Azure** and select **Barracuda Web Application Firewall - PAYG** or **Barracuda Web Application Firewall - BYOL** as per your requirement.

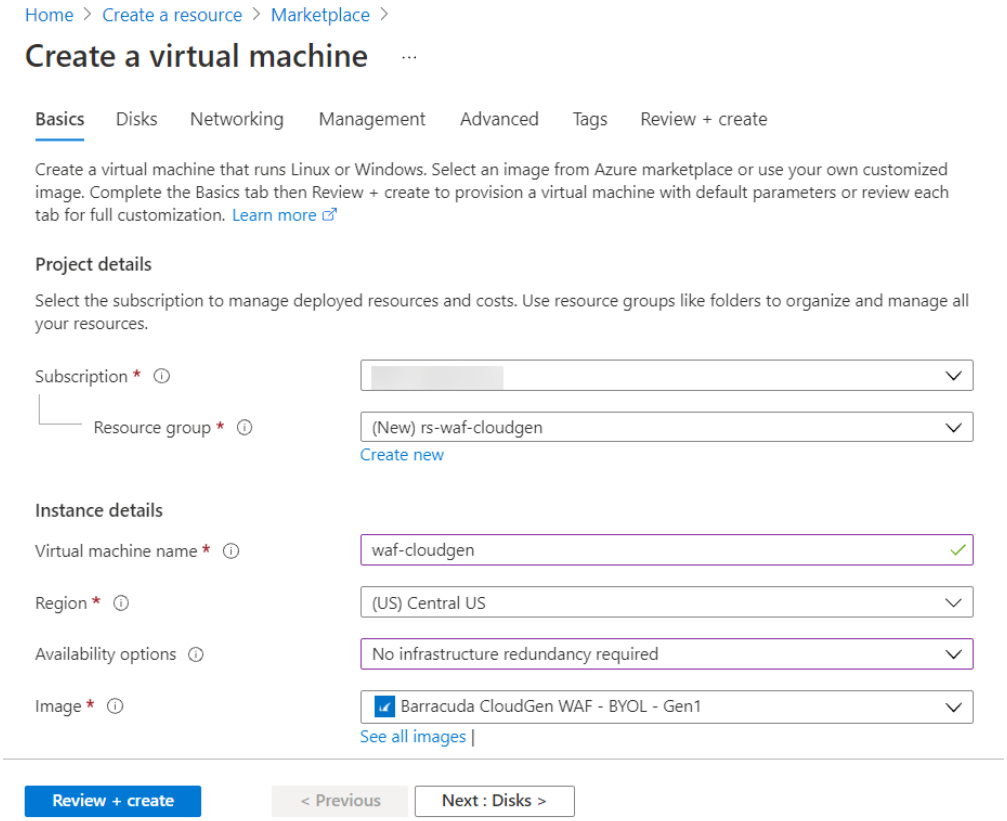


5. In the **Create a virtual machine**, **Basics** page:
    1. **Project details**
        1. **Subscription**: Select the subscription you want.
        2. **Resource group**: Create a new resource group, or select a resource group from the existing **Resource group** list.
    2. **Instance details**

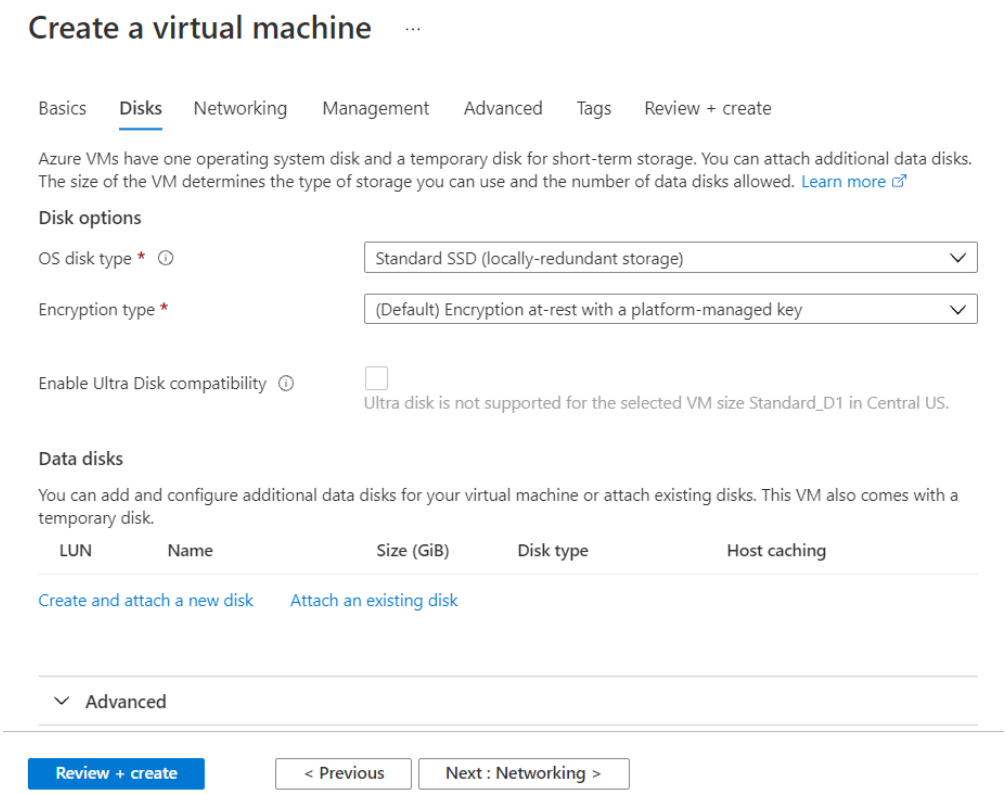
1. **Virtual machine name**: Enter a name for the virtual machine.
2. **Region**: Select the region where you want to deploy the virtual machine.
3. **Availability options**: Select the required option from the drop-down list.
4. **Image**: Keep the default.
5. **Size**: Select a size for the virtual machine.

3. **Administrator account**
   1. **Authentication type**: Choose **Password** and enter a password for the authentication. Note that this will be your password to access the Barracuda Web Application Firewall web interface.
   2. **Username**: Enter a username. Note: This entry is not used by the Barracuda Web Application Firewall.
   3. **Password**: Enter the password.
   4. **Confirm Password**: Re-enter the password.

6. Click **Next : Disks**.

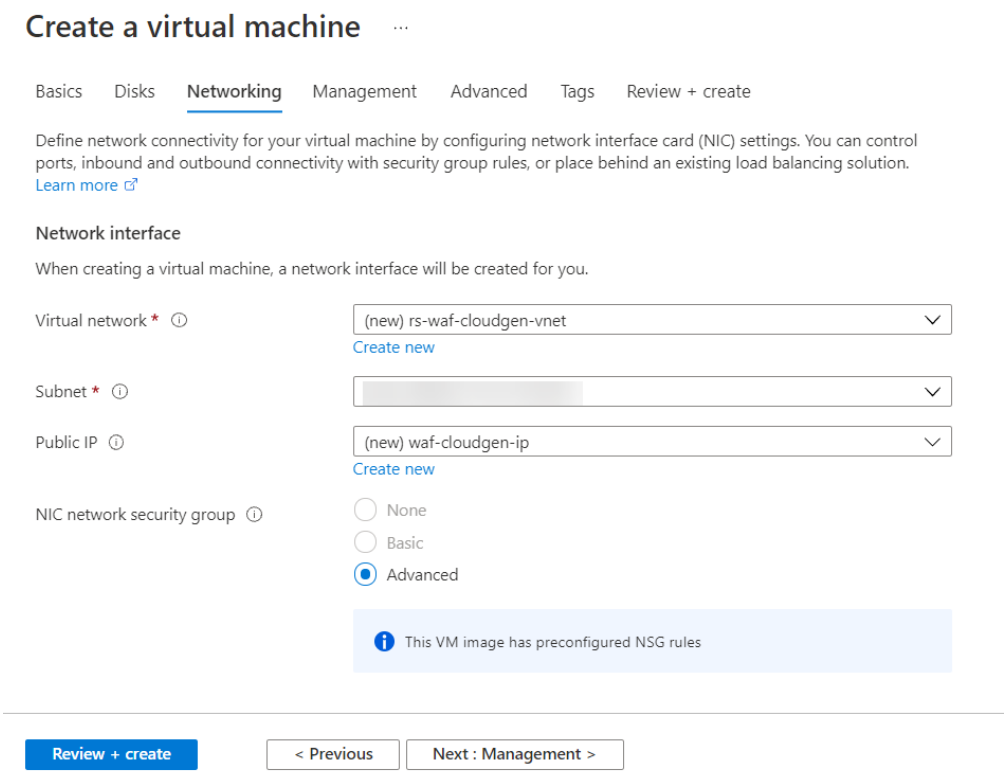


7. In the **Create virtual machine, Disks** page:
   1. Select the disk options and data disks as per your requirement.
8. Click **Next : Networking**.

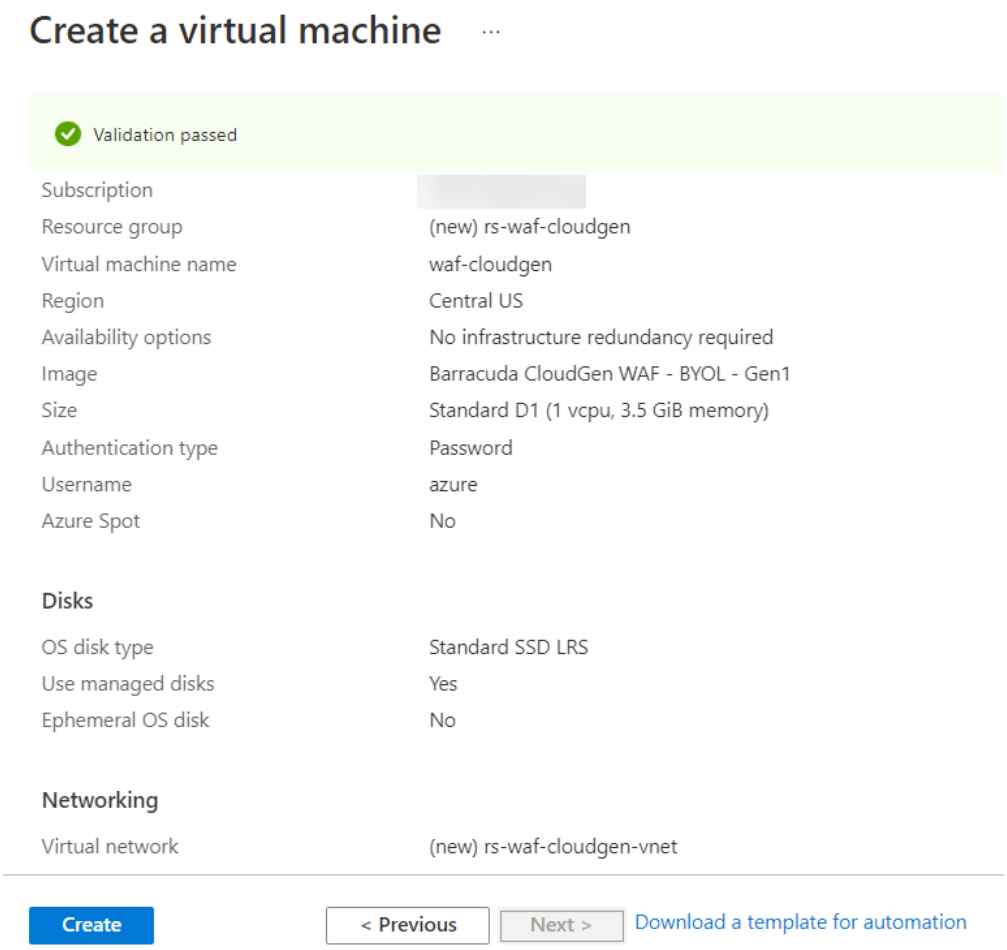


9. In the **Create virtual machine**, **Networking** page:
    1. **Network interface**
        1. **Virtual network**: Configure or select the network in which you want to deploy the Barracuda Web Application Firewall.
        2. **Subnet**: Configure or select the subnet in which you want to deploy the Barracuda Web Application Firewall.
        3. **Public IP**: Configure or select the public IP address to the Barracuda Web Application Firewall.
        4. **NIC network security group**: Keep the default value.
        5. **Configure network security group**: By default, port 8000 (TCP) and port 443 (TCP) will be opened as in your **Security Group** to access the web interface of the Barracuda Web Application Firewall. Configure additional rules that you want to use for creating services on the Barracuda Web Application Firewall.

            Microsoft Azure opens TCP/22 port by default in “Inbound security rules” under **Network security group** when the Barracuda Web Application Firewall is deployed. For security reasons, ensure it is deleted from the security group after the instance is deployed.
    2. **Load balancing**: Select the check box if you want to place the virtual machine behind an existing load balancing solution.
10. Click **Next : Management**.



11. In the **Create a virtual machine**, **Management** page:
    1. **Boot diagnostics**: Set the default values.
    2. Other configurations are not required.
12. Click **Next : Advanced**.
13. In the **Create a virtual machine**, **Advanced** page:
    1. No configuration is required..
14. Click **Next : Tags**.
15. In the **Create a virtual machine**, **Tags** page:
    1. Add the required tags and click **Next : Review + create**.
16. In the **Create a virtual machine**, **Review + create** page, review the configuration settings and click **Create**.



After you click **Create**, Microsoft Azure begins provisioning the Barracuda Web Application Firewall. You can check the status of the provisioned Barracuda Web Application Firewall from the Microsoft Azure Portal. Allow a few minutes before taking any further actions in the portal. During this time, the Microsoft Azure Linux Agent and Barracuda Web Application Firewall image boots up.

Do not restart the Barracuda Web Application Firewall while it is provisioning.

Next Step

Continue with the Barracuda Web Application Firewall Quick Start Guide - Microsoft Azure for licensing and initial configuration of your virtual machine**.**

Figures

1. Azure_services.png
2. Barracuda_CloudGen_WAF_for_Azure.png
3. Basics.png
4. Disks.png
5. Networking.png
6. Review.png