Barracuda Web Application Firewall Quick Start Guide - Microsoft Azure

https://campus.barracuda.com/doc/13861632/

Virtual machines (VMs) deployed through Azure Gallery prior to mid-February, 2015, do not support Disk Expansion. If you deployed prior to this time period and want to expand the disk, you must redeploy the VM using the latest VM image available in Azure Gallery:

- How to Add Additional Storage to Your Azure Deployment - New Portal

Before deploying the Barracuda Web Application Firewall for Azure, it is recommended that you go through the Deployment Best Practices article.

Step 1. Open Network Address Ranges on Firewall

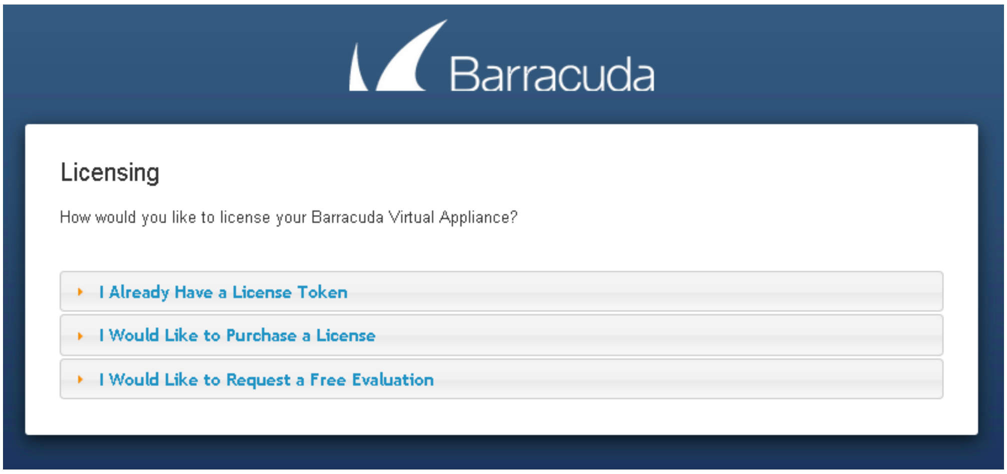
For more information on the list of Open Network Address ranges required for the firewall, refer to the Prepare for the Installation article.

Step 2. Licensing the Barracuda Web Application Firewall on Microsoft Azure

If you deployed the Barracuda Web Application Firewall with the **Hourly/Metered** option, you do not need to license the system; skip ahead to Step 3. "Verify Configuration and Change the Password".

After provisioning the Barracuda Web Application Firewall on Microsoft Azure, the next step is licensing. After you deploy the Barracuda Web Application Firewall image on the Microsoft Azure environment, do the following:

1. Sign into the Microsoft Azure Portal.
2. Note the DNS of the deployed Barracuda Web Application Firewall.
3. Open the browser and enter the noted DNS (from step 2) with port 8000 for HTTP and port 8443 for HTTPS. For example:
   For HTTP **:** http://<DNS>:8000
   For HTTPS **:** https://<DNS>:8443
   The Barracuda Web Application Firewall is not accessible via the HTTPS port when it is booting up. Therefore, use only the HTTP port to access the unit when booting. This displays the status of the unit, i.e., System Booting. After the boot process is complete, you will be redirected to the login page.
4. After the boot process is complete, the **Licensing** page displays with the following options:



Licensing

How would you like to license your Barracuda Virtual Appliance?

Barracuda
I Already Have a License Token
I Would Like to Purchase a License
I Would Like to Request a Free Evaluation

1. **I Already Have a License Token** – Use this option to provision your Barracuda Web Application Firewall with the license token you have already obtained from Barracuda Networks. Enter your Barracuda Networks token and default domain to complete licensing, and then click **Provision**.
   The Barracuda Web Application Firewall connects to the Barracuda Update Server to get the required information based on your license and then reboots automatically. Allow a few minutes for the reboot process. After the instance is provisioned, you are redirected to the login page.
2. **I Would Like to Purchase a License** – Use this option to purchase the license token for the Barracuda Web Application Firewall. Provide the required information in the form, accept the terms and conditions, and click **Purchase**.
   The Barracuda Web Application Firewall connects to the Barracuda Update Server to get the required information based on your license and then reboots automatically. Allow a few minutes for the reboot process. After the instance is provisioned, you are redirected to the login page.
3. **I Would Like to Request a Free Evaluation** – Use this option to get a 30-day free evaluation of the Barracuda Web Application Firewall. Provide the required information in the form, accept the terms and conditions, and click **Evaluate**.
   The Barracuda Web Application Firewall connects to the Barracuda Update Server to get the required information based on your license and then reboots automatically. Allow a few minutes for the reboot process. After the instance is provisioned, you are redirected to the login page.

Step 3. Verify Configuration and Change the Password

1. Log into the Barracuda Web Application Firewall web interface as the administrator using the URL as described in Step 3 of Licensing of Barracuda Web Application Firewall Vx after deploying on Microsoft Azure .

   Username: *admin*

   Password: Enter the password specified while deploying the Barracuda Web Application Firewall instance on the Microsoft Azure Management Portal. See Step **6.c** in the article *Deploying and Provisioning the Barracuda Web Application Firewall in the New Microsoft Azure Management Portal* .

2. Navigate to the **BASIC > Administration** page and do the following:
    1. **Old Password**: Enter the current password.
    2. **New Password**: (Optional) Enter a new password.
    3. **Re-enter New Password**: Re-enter the new password to confirm.
    4. Click **Save Password**.
3. Navigate to the **BASIC > IP Configuration** page and do the following:
    1. Verify the **WAN IP Configuration.**

       Do not make any changes in this section. This configuration is provided by Microsoft Azure and should not be changed.
    2. Configure the **Primary and Secondary DNS Server** in **DNS Configuration**.
    3. Enter **Default Host Name** and **Default Domain** in the **Domain Configuration**. The **Host Name** is used in reporting, and is displayed in alerts, notifications and messages sent by the Barracuda Web Application Firewall. The **Default Domain** is the domain for the system and is appended to the Host Name.

Step 4. Update the Firmware

Navigate to the **ADVANCED > Firmware Update** page and check if there is a new Latest General Release available. If so, perform the following steps to update the system firmware.

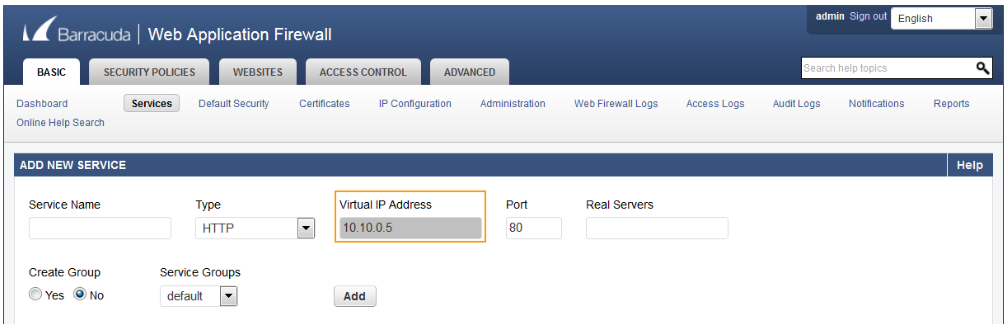
Make sure to read the release notes to learn about enhancements and new features before upgrading the firmware. It is also good practice to verify settings because new features may have been included with the firmware update.

1. Click on the **Download Now** button located next to the firmware version that you wish to install. When the download is complete, the **Apply Now** button appears.
2. Click on the **Apply Now** button to apply the firmware. This will take a few minutes to complete. After the firmware has been applied, the Barracuda Web Application Firewall will automatically reboot, displaying the login page when the system has come back up.
3. After applying the firmware, you will be required to log into the web interface of the Barracuda Web Application Firewall for Azure again.

It is recommended to use the **Capture** option to capture the Barracuda Web Application Firewall image, so that it can be used in case of disaster recovery (or other reason). For more information on how to capture the image, see Creating the Barracuda Web Application Firewall Image on Microsoft Azure.

Configure the Service(s) on the Barracuda Web Application Firewall

You can configure the services on the **BASIC > Services** page. The services should be created using the system (WAN) IP address of the instance as your virtual IP address (VIP). The **Virtual IP Address** field is thus automatically populated with the system (WAN) IP address of the instance. After the service is configured, the service will be accessible through the public IP/DNS of the Barracuda Web Application Firewall for Azure VM. Ensure that you have the corresponding ports opened in your security group/endpoints and firewall.



Service Name	Type	Virtual IP Address	Port	Real Servers
	HTTP	10.10.0.5	80	

Create Group: ○ Yes ● No

Service Groups: default

For more information on services, see Step 2: Configuring a Service. For detailed instructions on how to add a service, click the **Help** button.

Figures