Barracuda Web Security Gateway Vx Quick Start Guide

https://campus.barracuda.com/doc/6160412/

Use the steps in this article to set up your Barracuda Web Security Gateway Vx.

For Forward Proxy mode deployment limitations, refer to *Limitations of this Deployment Type* in the article Forward Proxy Deployment of the Barracuda Web Security Gateway .

Before You Begin

Deploy the Barracuda Web Security Gateway Vx on your hypervisor. You will only need a single virtual NIC on your virtual appliance.

Step 1. Configure Your Firewall

You need to configure your network firewall to allow ICMP traffic to outside servers as well as opening port 443 to `updates.cudasvc.com`. You also need to make sure that your DNS servers can resolve `updates.cudasvc.com`.

Step 2. Start the Virtual Appliance, Configure Networking, and Enter the License

You should have received your Barracuda Vx license token via email or from the website when you downloaded the Barracuda Web Security Gateway Vx package. If not, you can request an evaluation on the Barracuda website https://www.barracuda.com/purchase/evaluation or purchase one from https://www.barracuda.com/purchase/index. The license token looks similar to the following: 01234-56789-ACEFG.

1. In your hypervisor client, start the virtual appliance and allow it to boot up.
2. Log in to the console as *admin* with the password *admin.*
3. Arrow down to **TCP/IP Configuration**. Set the **System IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS Server**, and **Secondary DNS Server** for your virtual appliance. These fields can later be edited if needed from the **BASIC > IP Configuration** page in the product web interface.
4. Arrow down to **Licensing** and enter your Barracuda License Token and default domain to complete provisioning.

5. Arrow down to **Save Changes** and press Enter. The appliance will reboot at this time as a part of the provisioning process.
6. After the virtual appliance has finished rebooting, go to http://<your ip>:8000 to access the web interface and finalize configuration.

Step 3. Accept the End User License Agreement and Verify Configuration

1. Go to **http://<your ip>:8000** to access the web interface.
2. Read through the End User License Agreement. Scroll down to the end of the agreement.
3. Enter the required information: **Name**, **Email Address**, and **Company (if applicable)**. Click **Accept**. You are redirected to the Login page.
4. Log into the Barracuda Web Security Gateway Vx web interface as the administrator:
   Username: admin
   Password, which is either:

1. Go to the **BASIC > IP Configuration** page and enter values for **Default Hostname** and **Default Domain**. For example, enter *barracuda* as the **Default Hostname** and <yourcompanydomain.com> as the **Default Domain**. These names will be associated with anti-spyware email notification messages from the virtual appliance.
2. Note that, unlike the Barracuda Web Security Gateway appliance, there is no need or facility to set **Operating Mode** for the Barracuda Web Security Gateway Vx. This is because, in Forward Proxy deployment, *Audit* mode works just like *Active* mode; traffic is logged and policies are applied.
3. Click the **Save Changes** button to save all of the information.

Step 4. Update the Firmware

Navigate to the **Advanced > Firmware Update** page. If there is a new *Latest General Release* available, perform the following steps to update the system firmware:

1. Click on the **Download Now** button located next to the firmware version that you wish to install. To view download progress, click on the **Refresh** button. When the download is complete, the **Refresh** button will be replaced by an **Apply Now** button.
2. Click on the **Apply Now** button to install the firmware. This will take a few minutes to complete.
3. After the firmware has been applied, the Barracuda Web Security Gateway Vx will automatically reboot, displaying the login page when the system has come back up.
4. Log back into the web interface again and read the Release Notes to learn about enhancements and new features. It is also good practice to verify settings you may have already entered, as new features may have been included with the firmware update.

Step 5. Update the Category Definitions

Barracuda recommends that you update the web content category definitions on a newly installed Barracuda Web Security Gateway Vx (this step is not necessary on a physical appliance). The content categories are used to block web sites.

Navigate to the **ADVANCED > Energize Update** page.

1. Scroll down to the **Category Definitions Update** section.
2. Click **Update** to get the latest web category definitions.

Step 6. Change the Administrator Password

To avoid unauthorized use, we recommend you change the default administrator password to a more secure password. You can only change the administrator password for the Web interface. Go to the **BASIC > Administration** page and enter your old and new passwords, then click on **Save Password**.

Next Step

Continue with Directing Traffic to the Barracuda Web Security Gateway Vx. See also Allocating Cores, RAM, and Hard Disk Space for Your Barracuda Web Security Gateway Vx.