Barracuda Email Security Gateway Vx Quick Start Guide

https://campus.barracuda.com/doc/3866625/

Before You Begin

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

Step 1. Open Network Address Ranges and Ports on Firewall

If your Barracuda Email Security Gateway Vx is located behind a firewall, open the following Barracuda network address ranges for the ports shown in the table below on your firewall to ensure proper operation:

- 64.235.144.0/20
- 209.222.80.0/21

Port	Direction	TCP	UDP	Usage
22/8788	Out	Yes	No	Technical Support Services
25	In/Out	Yes	No	Email and email bounces
53	Out	Yes	Yes	Domain Name Service (DNS). Verify that the DNS servers can resolve `updates.cudasvc.com.`
80	Out	Yes	No	Virus, firmware, and spam rule updates
123	Out	No	Yes	Network Time Protocol (NTP)
443	Out	Yes	No	HTTPS/SSL port used for initial VM provisioning and access to `updates.cudasvc.com`*
*You can disable the initial provisioning port after the initial provisioning process is complete.				

When deploying the Barracuda Email Security Gateway Vx, you must also configure your firewall to allow ICMP traffic from the Barracuda Email Security Gateway Vx to outside servers.

Step 2. Start Your Virtual Appliance, Configure the Network Settings, and Enter the License

You should have received your Barracuda Vx license token via email or from the website when you downloaded the Barracuda Email Security Gateway Vx package. If not, you can request an evaluation

on the Barracuda website at 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. Log in to the console as **admin** with the password **admin**.
2. Navigate to **TCP/IP Configuration**.
3. Enter the following IP information (you can edit these fields later on the **BASIC > IP Configuration** page in the product web interface):
   - **IP Address** - This IP address identifies the Barracuda Email Security Gateway Vx to your organization's network.
   - **Netmask** - The sub-network mask (subnet mask or netmask) provides a simple way to limit which other devices on the network can access the Barracuda Email Security Gateway Vx directly.
   - **Default Gateway** - The default gateway is the internal network device the Barracuda Email Security Gateway Vx connects to to reach the parts of the internal network it cannot access directly within its subnet.
   - **Primary DNS Server** - The primary domain name system (DNS) server contains a database of network device names and their corresponding Internet address hosts. DNS servers allow you to identify devices by name instead of by address.
   - **Secondary DNS Server** - The secondary DNS server acts as a backup to the primary.
4. Under **Licensing** enter your Barracuda License **Token** and **Default Domain** to complete provisioning. The appliance will reboot as a part of the provisioning process.

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

1. Go to **http://<configured IP address for the Barracuda Email Security Gateway>: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 Email Security Gateway Vx web interface as the administrator: **Username**: `admin` **Password**: `admin`
5. Go to the **BASIC > IP Configuration** page and verify that the following settings are correct:
   - **IP Address**
   - **Subnet Mask**
   - **Default Gateway**
   - **Primary DNS Server**
   - **Secondary DNS Server**
6. Enter the **Server Name/IP** of the destination email server where you want the Barracuda Email Security Gateway Vx to deliver mail.
   For example: type: *mail.<yourdomainname>.com*
7. Enter the **Default Hostname**.
   For example: *<yourhost>*

The host name is added to bounce messages.
8. Enter the **Default Domain**.
   For example: *<yourcompanydomain.com>*
   The domain is added to bounce messages and reports.
9. Under **Allowed Email Recipient Domain(s)**, enter each domain for which you want the Barracuda Email Security Gateway Vx to receive email.
   The Barracuda Email Security Gateway Vx rejects all incoming email that is addressed to domains that are not specified here.

Step 4. Update the Firmware

The product Firmware is the software running all of the features and functions on the Barracuda Email Security Gateway Vx.

Firmware updates always require a reboot of the Barracuda Email Security Gateway Vx. To minimize interruptions, Barracuda Networks recommends updating the firmware after peak business hours.

Go to the **ADVANCED > Firmware Update** page. Compare the **Current Installed Version** to the **Latest General Release**. If there is a new **Latest General Release** available, perform the following steps to update the system firmware:

1. Click **Download Now** next to the firmware version that you want to install. To view the download progress, click **Refresh**. When the download is complete, the **Refresh** button is replaced by the **Apply Now** button.
2. Click **Apply Now** to install the firmware. The firmware installation takes several minutes to complete.
   After the firmware is applied, the Barracuda Email Security Gateway Vx automatically reboots. The login page is displayed when the system comes back up.
3. Log back into the web interface and read the Release Notes to learn about enhancements and new features. It is also good practice to verify settings that you have already entered, because new features might have been included with the firmware update.

For more information, see Product Activation and Update Firmware.

Step 5. Change the Administrator Password

To prevent unauthorized use, change the default administrator password to a more secure password. Go to the **BASIC > Administration** page, enter your old and new passwords, and click **Save**

Password. This changes the administrator password for the web interface.There is also a separate administrator account for the console. This password can be changed as well by navigating to **System** and entering the old and new passwords.

Step 6. Verify the Barracuda Email Security Gateway Vx Configuration

After you install your Barracuda Email Security Gateway Vx and configure your firewall, you can test the configuration. Go to the **ADVANCED > Troubleshooting** page. In the **Network Connectivity Tests** section, enter `updates.cudasvc.com` in the **Ping Device** box and click **Begin Ping**. The Barracuda Email Security Gateway sends ping packets to the `updates.cudasvc.com` server. The results are displayed in a popup window. If your Vx is able to transmit and receive all of the ping packets without packet loss, your virtual appliance is configured correctly to access the Internet.

Next Step

Your Barracuda Email Security Gateway Vx is now activated, able to send and receive network traffic, and is running the latest firmware. You're ready to begin setting up the Vx to filter spam, viruses, malware, and spyware from incoming email. To begin this configuration, go to Configure the Web Interface .