Barracuda SSL VPN Vx Quick Start Guide

https://campus.barracuda.com/doc/39813722/

After your virtual appliance has been deployed, you must provision it. You need your Barracuda Vx license token, which you received via email or from the website when you downloaded the Barracuda SSL VPN Vx package. The license token is a 15 character string, formatted like this: `01234-56789-ACEFG`.

Before you begin

Deploy the Barracuda SSL VPN Vx on your hypervisor. For more information, see How to Deploy Barracuda SSL VPN Vx Images.

Step 1. Open firewall ports

If your Barracuda SSL VPN Vx is located behind a corporate firewall, open the following ports on your firewall to ensure proper operation:

Port	Protocol	Direction	Usage
22	TCP	Out	Remote diagnostics and service (recommended)
25	TCP	Out	Email alerts and one-time passwords
53	TCP/UDP	Out	DNS
80	TCP	Out	Energize Updates
123	UDP	Out	Network Time Protocol (NTP)
443	TCP	In/Out	HTTPS/SSL port for SSL VPN access and Initial VM Provisioning
8000	TCP	In/Out	External appliance administrator port (HTTP)
8443	TCP	In/Out	External appliance administrator port (HTTPS)

If PPTP or L2TP/IPsec access is required, also open the following ports:

Port	Protocol	Direction	Usage
47	GRE	In/Out	PPTP
1723	TCP	In	PPTP
500	UDP	In	L2TP/IPsec
4500	UDP	In	L2TP/IPsec

Note: Only open the appliance administrator interface ports on 8000/8443 if you intend to manage the appliance from outside the corporate network.

Configure your network firewall to allow ICMP traffic to outside servers, and open port 443 to `updates.barracudacentral.com`. You must also verify that your DNS servers can resolve `updates.barracudacentral.com` from the Internet.

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 SSL VPN 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. In your hypervisor client, start the virtual appliance and allow it to boot up.
2. From the console, log in with the following credentials:
    - **Username**: `admin`
    - **Password**: enter the serial number of your Barracuda SSL VPN.

      This default password is intended for initial access only. You must change it once you have configured your Barracuda SSL VPN. For more information, see Step 5 in this article.
3. In the **System Configuration** window, use the down arrow key and select **TCP/IP Configuration**. Configure the following:
    - WAN IP Address
    - WAN Netmask
    - Gateway Address
    - Primary DNS Server
    - Secondary DNS Server
4. If the Internet can be accessed only through an explicit proxy, configure the proxy server using **Proxy Server Configuration (Optional)**, so that it reaches the Internet for provisioning.
5. 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 the 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 SSL VPN Vx web interface as administrator:

- **Username**: `admin`
- **Password**: enter the serial number of your Barracuda SSL VPN.

5. Go to the **BASIC > IP Configuration** page and verify that the following settings are correct:
    - **IP Address**, **Subnet Mask**, and **Default Gateway**.
    - **Primary DNS Server** and **Secondary DNS Server**.
    - (If you are using a proxy server on your network) **ProxyServer Configuration**.

Step 4. Update the firmware

Go 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 **Download Now** next to the firmware version that you want to install.
2. When the download finishes, click **Apply Now** to install the firmware. The firmware installation takes a few minutes to complete.
   After the firmware has been applied, the Barracuda SSL VPN Vx automatically reboots. The login page displays when the system has come back up.
3. Log back into the web interface, and read the Release Notes to learn about enhancements and new features.

For more information, see Update Firmware.

Step 5. Change the administrator password for the appliance web interface

To prevent unauthorized use, you must change the default administrator password to a more secure password. Go to the **BASIC > Administration** page, enter your old and new passwords, and then click **Save Password**. This only changes the password for the appliance web interface. The password for the ssladmin user on the SSL VPN web interface must be changed separately.

Step 6. Route incoming SSL connections to the Barracuda SSL VPN Vx

Route HTTPS incoming connections on port 443 to the virtual appliance. This is typically achieved by configuring your corporate firewall to port forward SSL connections directly to the Barracuda SSL VPN Vx.

Ports for Remote Appliance Management

If you are managing the virtual appliance from outside the corporate network, the appliance administrator web interface ports on 8000/8443 need similar port forward configurations. Barracuda Networks recommends that you use the appliance web interface on port 8443 (HTTPS).

Step 7. Verify incoming SSL connections to the Barracuda SSL VPN Vx

After you configure your corporate firewall to route SSL connections to the Barracuda SSL VPN Vx, verify that you can accept incoming SSL connections.

1. Test the connection by using a web browser from the Internet (not inside the LAN) to establish an SSL connection to the external IP address of your corporate firewall. For example, if your firewall's external IP address is 23.45.67.89, go to `https://23.45.67.89` in your browser.
2. When you are prompted to accept an untrusted SSL certificate, accept the warning and proceed to load the page.
   If you see the Barracuda SSL VPN login screen, this confirms that your appliance can receive connections from the Internet.

Next step

Configure your virtual machine. For instructions, see Getting Started.