Barracuda SSL VPN - Quick Start Guide

The Barracuda SSL VPN provides remote users secure, clientless access to your internal network. The Barracuda SSL VPN may be installed directly inside the LAN or in a more complex DMZ configuration. Follow the instructions in this guide to configure the Barracuda SSL VPN to accept incoming connections from the Internet.

1 Getting Started

To begin setting up your Barracuda SSL VPN, you will need the following:

- Barracuda SSL VPN appliance
- AC power cord; AC input voltage range is 100-240 volts at 50/60 Hz
- Ethernet cables
- VGA monitor (recommended)
- PS2 keyboard (recommended)

2 Physical Installation

1. Install the Barracuda SSL VPN to a 19-inch rack or place it in a stable location.
2. Connect an Ethernet cable from your network switch to the Ethernet port on the back of the Barracuda SSL VPN.
3. Connect a VGA monitor, PS2 keyboard, and the AC power cord to the unit.
4. Turn on the unit by pressing the power button on the front panel.

3 Configure IP Address and Network Settings

With a monitor and keyboard attached

As soon as the Barracuda SSL VPN is fully booted the administrative console login is displayed:

1. Log into the Administrative Console using the admin credentials:

   Login: admin
   Password: admin

2. Configure the **IP Address, Subnet Mask, Default Gateway, Primary DNS Server** and **Secondary DNS Server** as appropriate for your network.

Without a monitor and keyboard attached

Use the RESET button on the front panel to configure the IP adress. Press and hold the RESET button according to the table bellow:

IP Address	Netmask	Press and hold RESET for
192.168.200.200	255.255.255.0	5 seconds
192.168.1.200	255.255.255.0	8 seconds
10.1.1.200	255.255.255.0	12 seconds

4 Configure the Firewall

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

Port	Direction	TCP	UDP	Usage
22	Out	Yes	No	Remote diagnostics and service (recommended)
25	Out	Yes	No	Email alerts + One-time passwords
53	Out	Yes	Yes	Domain Name Service (DNS)
80	Out	Yes	No	Firmware and definition updates
123	Out	No	Yes	Network Time Protocol (NTP)
443	In	Yes	No	HTTPS/SSL port for SSL VPN access
8000	Out	Yes	No	Firmware and definition updates (backup)

Typically the corporate firewall is configured to port forward incoming HTTPS/SSL connections on port 443 directly to the Barracuda SSL VPN.

Port	Direction	TCP	UDP	Usage
1723	In	Yes	No	**PPTP** access (**PPTP** access also requires GRE (IP protocol 47))
500	In	No	Yes	**L2TP/IPsec** access
4500	In	No	No	**L2TP/IPsec** access

To use L2TP/IPsec and PPTP in combination with an internal firewall, you must open the following ports:

Port	Direction	TCP	UDP	Usage
389	Out	Yes	No	LDAP/Active Directory read access
636	Out	Yes	No	LDAP/Active Directory read/write access

5 Log into the Appliance Web Interface

Use a computer with a web browser that is connected to the same network as the Barracuda SSL VPN, to log into the web interface:

1. Enter *http://IP address of the Barracuda SSL VPN:default appliance web interface HTTP port* in your browser. For example, if you configured the Barracuda SSL VPN with an IP address of 192.168.200.200, you would type: http://192.168.200.200:8000
2. Log into the appliance web interface as the administrator: **Login:** admin , **Password:** admin

6 Confirm the Network Settings

1. Go to the **BASIC > IP Configuration** page to verify your settings:
   - Verify the **IP Address, Subnet Mask**, and **Default Gateway**.
   - Verify the **Primary and Secondary DNS Server**.
   - Enter the **Default Hostname** and **Default Domain**.
   - If you are using a proxy server on your network, verify the Proxy Server Configuration settings
2. Complete the rest of the fields on this page and save your changes.

7 Complete the Product Activation

If a warning message is displayed at the top of every page on the Barracuda SSL VPN appliance web interface, activate the Barracuda SSL VPN by following these steps:

1. Click on the link in the warning message or use the link on the **BASIC > Status** page to open the **Barracuda Networks Product Activation** page in a new browser window.
2. Fill in the required fields and click **Activate**. A confirmation page opens, displaying the terms of your subscription.

8 Update the Firmware

Barracuda Networks recommends to use the Latest General Release. You can update by visiting the **ADVANCED > Firmware Update** page and following these steps:

1. Click **Download Now**. You will be notified when the download is complete.
2. Click **Apply Now** to apply the firmware. This takes a few minutes.
3. The system will automatically reboot and prompt you to log in, after the firmware is applied.

9 Change the Administrator Password

To avoid unauthorized use, change the default appliance administrator password.

1. Go to **BASIC > Administration** page and change your password.
2. Complete the rest of the fields on this page.
3. Click **Save Changes**.

10 Verify Incoming Connections to the Barracuda SSL VPN

The Barracuda SSL VPN is able to accept incoming SSL connections, once your corporate firewall is configured to forward SSL connections through to the Barracuda SSL VPN.

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 203.0.113.1, direct your browser to https://203.0.113.1/
2. Proceed at the certificate warning.
3. On the login page for the SSL VPN web interface, log in with the default credentials for the SSL VPN administrator:

Login: ssladmin
Password: ssladmin

Now you can set up accounts and other resources for users of the Barracuda SSL VPN.

Next Steps

- Obtain a trusted certificate signed by a third party Certification Authority (CA) for the Barracuda SSL VPN.
- Register a hostname with your DNS server for the Barracuda SSL VPN

For Barracuda Firewall technical documentation, visit

http://techlib.barracuda.com/SSLVPN