

Step 3 - Initial Configuration

<https://campus.barracuda.com/doc/3866720/>

Configure IP Address and Network Settings

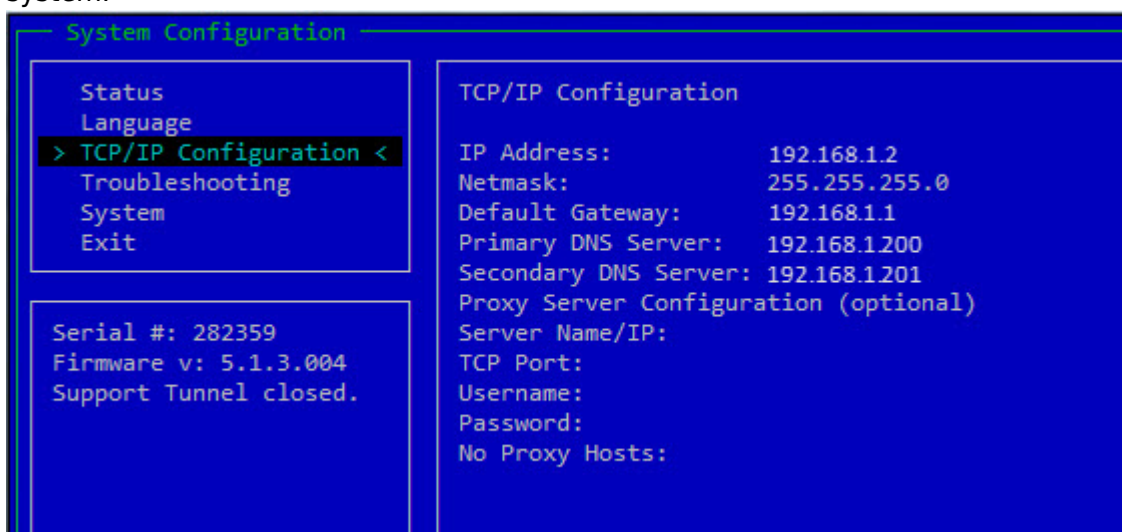
The Barracuda Email Security Gateway is given a default IP address of 192.168.200.200. You can change this address by doing either of the following:

- Connect directly to the Barracuda Email Security Gateway with a keyboard and monitor and specify a new IP address through the console interface.
- Log into the Barracuda Email Security Gateway web interface as *admin* and change the IP address on the **BASIC > IP Configuration** page. See **Configure the Barracuda Email Security Gateway From the Web Interface** below for details.

To connect directly to the Barracuda Email Security Gateway to set a new IP address:

1. At the **barracuda login** prompt, enter *admin* for the login and, for the password:
If your appliance serial number is higher than **1311431**, then the default administrator password is the numeric portion of the serial number. If your serial number is **1311431** or lower, then the default administrator password is **admin**. For help finding the serial number of your appliance, see [Serial Number for Hardware and Virtual Appliances](#).

The **User Confirmation Requested** window will display the current IP configuration of the system.



```
System Configuration
├── Status
├── Language
├── > TCP/IP Configuration <
├── Troubleshooting
├── System
├── Exit
├── Serial #: 282359
├── Firmware v: 5.1.3.004
├── Support Tunnel closed.
└── TCP/IP Configuration
    ├── IP Address: 192.168.1.2
    ├── Netmask: 255.255.255.0
    ├── Default Gateway: 192.168.1.1
    ├── Primary DNS Server: 192.168.1.200
    ├── Secondary DNS Server: 192.168.1.201
    ├── Proxy Server Configuration (optional)
    ├── Server Name/IP:
    ├── TCP Port:
    ├── Username:
    ├── Password:
    └── No Proxy Hosts:
```

2. Using the Tab key, select **Yes** to change the IP configuration.
3. Enter the new IP address, netmask, and default gateway for your Barracuda Email Security Gateway, and select **OK** when finished.
4. Select **No** when prompted if you want to change the IP configuration. Upon exiting the screen, the new IP address and network settings will be applied to the Barracuda Email Security

Gateway.

Configure Your Corporate Firewall

If your Barracuda Email Security Gateway is located behind a corporate firewall, you need to open specific ports to allow communication between the Barracuda Email Security Gateway and remote servers. See also [Required Outbound Connections for Barracuda Networks Appliances](#).

To configure your corporate firewall:

- Using the following table as a reference, open the specified ports on your corporate firewall:

Port	Direction	Protocol	Used for
22	Out	TCP	Remote diagnostics and technical support services (recommended). If you don't want to leave this port open, you can just open for technical support sessions if needed, and then close the port again after the session.
25	In/Out	TCP	SMTP
53	Out	TCP/UDP	Domain Name Server (DNS)
80 ⁽¹⁾	Out	TCP	Virus, firmware, security and spam rule definitions
123	Out	UDP	NTP (Network Time Protocol)
8000 ⁽²⁾ (default)	Out	TCP	Virus, firmware, security and spam rule definitions
443	Out	TCP	Optional : Allow access to HTTPS links in emails.

Notes:

⁽¹⁾ If your firewall allows unrestricted outbound traffic on port 80, then no further action is necessary. If there are restrictions on outbound traffic on this port, you must configure your firewall as described in [Required Outbound Connections for Barracuda Networks Appliances](#) to allow the Barracuda Email Security Gateway access to firmware and definition updates.

⁽²⁾ If your firewall allows unrestricted outbound traffic on port 8000, then no further action is necessary.

- If appropriate, change the NAT routing of your corporate firewall to route incoming email to the Barracuda Email Security Gateway. Consult your firewall documentation or your corporate firewall administrator to make the necessary changes.

After specifying the IP address of the system and opening the necessary ports on your firewall, you need to configure the Barracuda Email Security Gateway from the web interface. Make sure the computer from which you configure the Barracuda Email Security Gateway is connected to the same network, and the appropriate routing is in place to allow connection to the Barracuda Email Security

Gateway's IP address from a web browser.

Configure the Barracuda Email Security Gateway From the Web Interface

1. From a web browser, enter the IP address of the Barracuda Email Security Gateway followed by port 8000.
Example: `http://192.168.200.200:8000`
2. Log in to the web interface using *admin* for the username and, for the password:
 - If your appliance serial number is higher than **1311431**, then the default administrator password is the numeric portion of the serial number. For help finding the serial number of your appliance, see [Serial Number for Hardware and Virtual Appliances](#).
 - If your serial number is **1311431** or lower, then the default administrator password is *admin*.**For maximum security, version 9.2 and higher requires changing the administrator password before proceeding.**
3. On the **BASIC > IP Configuration** page, enter the required information in the fields as described in the following table:

Fields	Description
TCP/IP Configuration	The IP address, subnet mask, and default gateway of your Barracuda Email Security Gateway. The TCP port is the port on which the Barracuda Email Security Gateway receives incoming email. This is usually port 25.
Destination Mail Server TCP/IP Configuration	The hostname or IP address of your destination mail server; for example <i>mail.yourdomain.com</i> . This is the mail server that receives email after it has been checked for spam and viruses. You should specify your mail server's hostname rather than its IP address so that the destination mail server can be moved and DNS updated at any time without any changes needed to the Barracuda Email Security Gateway. TCP port is the port on which the destination mail server receives all SMTP traffic such as inbound email. This is usually port 25. If you need to set up more than one domain or mail server, refer to Creating and Managing Domains .
DNS Configuration	The primary and secondary DNS servers you use on your network. It is strongly recommended that you specify a primary and secondary DNS server. Certain features of the Barracuda Email Security Gateway rely on DNS availability.
Domain Configuration	Default Host Name is the host name to be used in the reply address for email messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Email Security Gateway. The Default Host Name is appended to the default domain. Default Domain is a required field and indicates the domain name to be used in the reply address for email messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Email Security Gateway.

Accepted Email Recipients Domains	The domains managed by the Barracuda Email Security Gateway. Make sure this list is complete. The Barracuda Email Security Gateway rejects all incoming messages addressed to domains not in this list. See Creating and Managing Domains . Note: One Barracuda Email Security Gateway can support multiple domains and mail servers. If you have multiple mail servers, go to the DOMAINS tab and enter the mail server associated with each domain
-----------------------------------	--

4. Click **Save**.

If you changed the IP address of your Barracuda Email Security Gateway, you are disconnected from the web interface and will need to log in again using the new IP address.

If You Have a Model 100

Go to the **Users** page and perform *at least one* of the following:

- Enter the email address(es) on which the Barracuda Email Security Gateway is to perform spam and virus scanning under **User Configuration**, one entry per line.
- To have email addresses automatically added to the Barracuda Email Security Gateway as mail arrives, make sure the **Enable User Addition** option is turned on.

Note: If no users are specified, *AND* the Enable User Addition option is set to No, then no scanning of *ANY* incoming email will be performed.

Continue with [Step 4 - Product Activation and Firmware Update](#)

Figures

1. ConsoleScreenshot.JPG

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.