Getting Started

https://campus.barracuda.com/doc/73702144/

When deploying a Barracuda CloudGen Firewall, basic settings must be made before the firewall can be used. There are some differences, depending on the deployment option you choose (hardware or public cloud). Stand-alone hardware models up to the F400 running a fresh 7.1.0 installation use the web interface as the default management interface. You can change this during the setup process.

Before You Begin

Make sure you complete the steps listed in the deployment articles, depending on which platform you are deploying the firewall on:

- **Hardware** – Complete Hardware deployment and the included Quick Start Guide. The Quick Start Guide is included in the box with every firewall. Your PC must be connected to the management port of the CloudGen Firewall and use an IP address in the 192.168.200.0/24 range. Do not use 192.168.200.200. This IP address is the default management IP address of the firewall.
- **Public Cloud** – Complete the steps in Public Cloud for your public cloud provider.

Step 1. Log into the Web Interface

Log into the web interface with the default user credentials of your deployment:

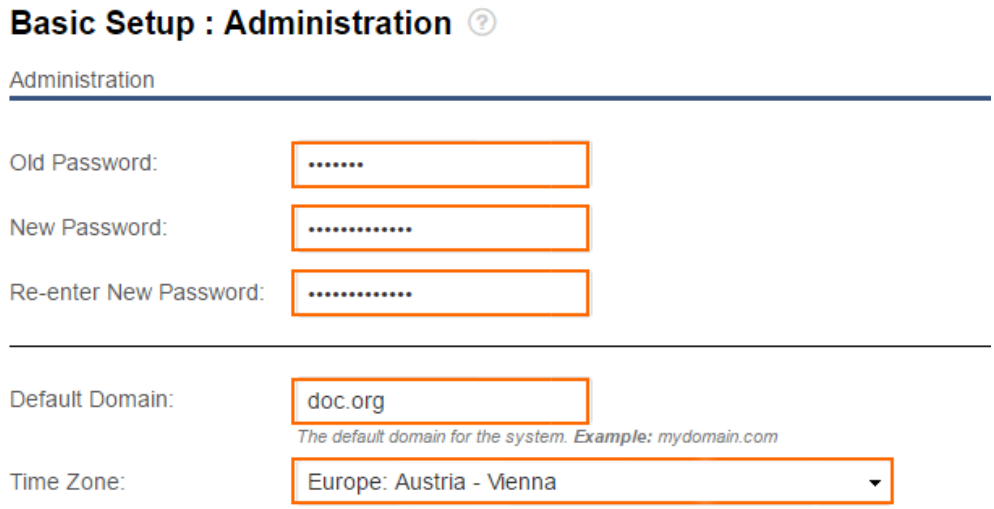
The default password *ngf1r3wall* is intended for initial access only. You must change the password once you are logged into the appliance.

	Management IP Address	Username	Default Password
Hardware	192.168.200.200	root	ngf1r3wall
Public Cloud - Amazon AWS	Elastic IP pointing to the Barracuda CloudGen Firewall instance	root	Instance ID of your Barracuda CloudGen Firewall instance. E.g., **i-0aaaa123**
Public Cloud - Microsoft Azure	***<your cloud service>*.cloudapp.net** or Virtual IP (VIP) for the cloud service	root	• Set during deployment • If not set during deployment: ngf1r3wall
Public Cloud - Google Cloud	Static external IP address assigned to the firewall instance	root	Name of the instance

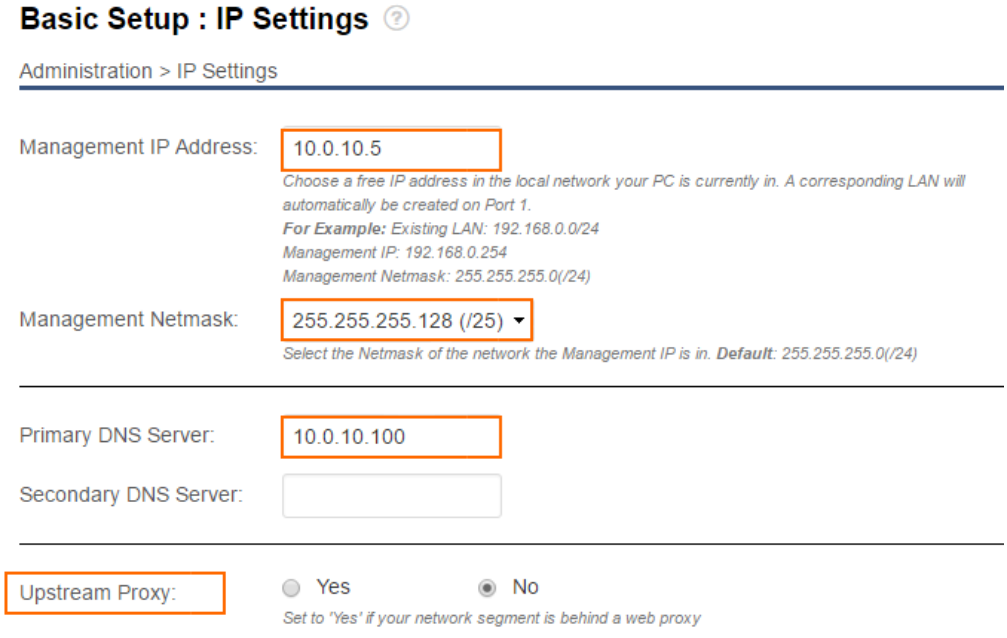
Step 2. Complete the Basic Setup Wizard

The basic setup wizard automatically starts when you first log into the firewall.

1. Change the **Password**.
2. Enter the **Default Domain** for your network.
3. Select the **Time Zone**.



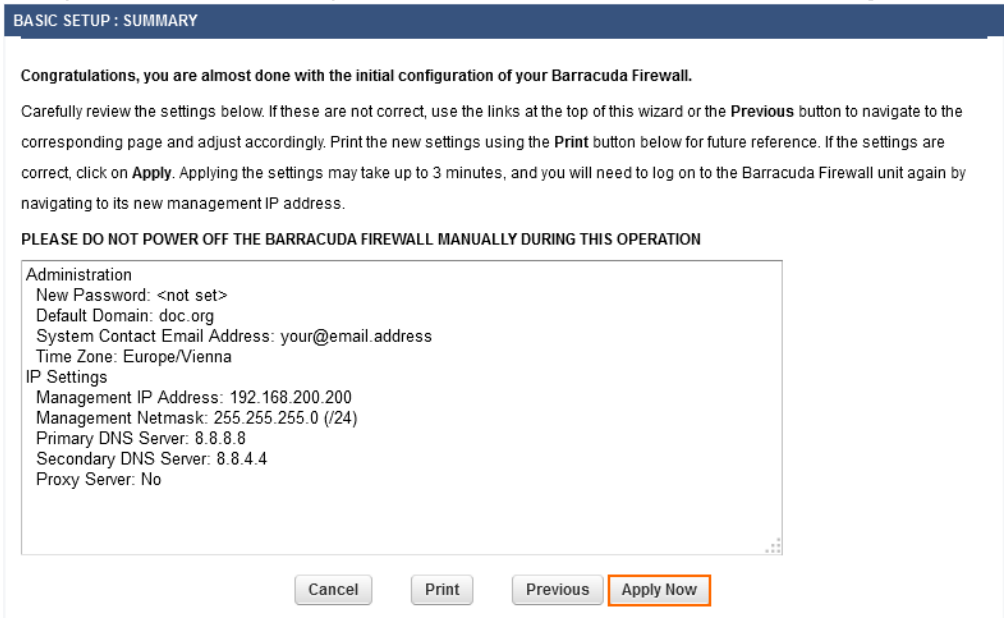
4. Click **Next**.
5. (optional) Change the **Management IP Address** to match your existing network.
6. (optional) Change the **Management Netmask** to match the management network.
7. Enter the **Primary** and **Secondary DNS Server**.



8. (optional) If the network segment connected to **P2** requires an HTTP proxy to access the Internet, set **Upstream Proxy** to **Yes**.

- **Proxy Server** – Enter the IP address of your proxy server.
- **Proxy Port** – Enter the port the proxy server is listening on. E.g., 3128
- **(optional) Proxy Username** – Enter the username used to authenticate to the proxy.
- **(optional) Proxy Password** – Enter the proxy password.

9. Complete the activation process and click **Next**. The **Basic Setup: Summary** window opens.

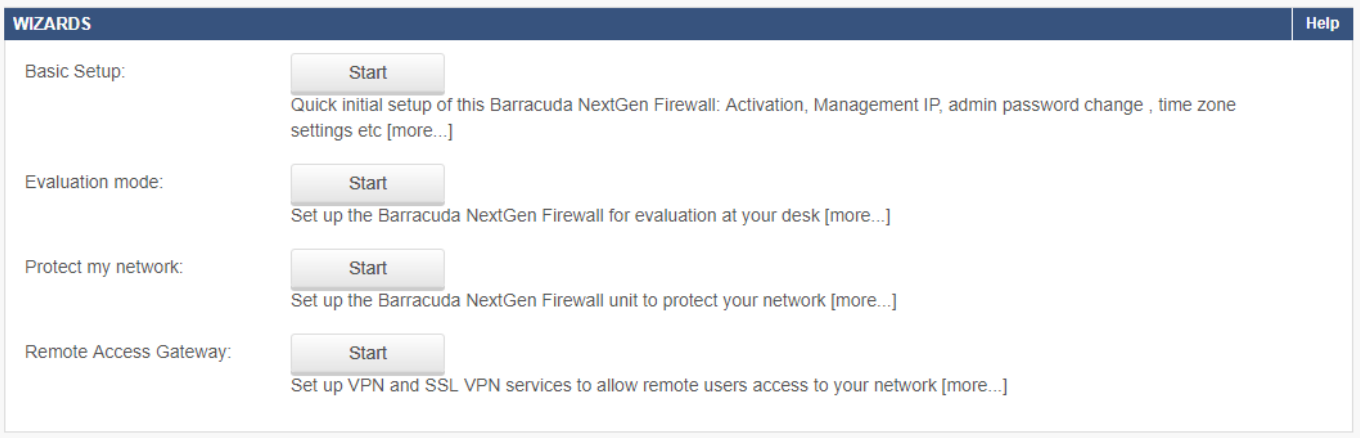


10. Review your configuration settings.
11. (optional) Click **Print** .
12. Click **Apply Now**.

    If you changed the time zone, the firewall will now reboot.

Next Step

After the reboot, select a wizard for a customized setup, or configure the appliance manually. To start the wizards, go to **ADVANCED > Wizards**.



Configure the CloudGen Firewall as a Firewall

Configure the CloudGen Firewall as a firewall by completing the configuration wizard matching your use case.

For more information, see Deploy as Firewall.

Configure the CloudGen Firewall as a Remote Access Gateway

Configure the CloudGen Firewall as a remote access gateway by using the Remote Access Gateway wizard. This wizard takes you through the necessary steps to configure a client-to-site VPN.

For more information, see Deploy as Remote Access Gateway.

Figures

1. wizard_01a.png
2. wizard_02.png
3. wizard_04.png
4. wizards.png