

Deploy as Firewall

<https://campus.barracuda.com/doc/53676483/>

The initial setup wizard automatically starts when you first log into the firewall and guides you through the first configuration steps. Use the wizards to deploy the firewall into production or to evaluate it.

You can also start the wizards at a later time: Go to **ADVANCED > Wizards**.

Step 1. Complete the setup wizard

The initial setup wizard automatically starts when you first log into the firewall. (When using another wizard, go to **ADVANCED > Wizards**, and click **Start** to launch the wizard.)

- **Evaluation mode** – Sets up the firewall for evaluation at your desk or in a test lab. All network traffic is transparently forwarded from network interface p1 to p3. Verify p1 is connected to your LAN, and p3 to your test PC or test network.
- **Protect my network** – Configures a primary and a secondary Internet uplink as well as up to two internal networks, including DHCP server configuration. To complete this, wizard the following information is required:
 - Local area network preferences (LAN IP address, gateway IP address, required DHCP settings)
 - Internet service provider (ISP) uplink information
 - Failover Internet service provider information (optional)
- **Manual configuration** – Click **Close** to exit the setup wizard.

Step 2. Configure administrator IP/range

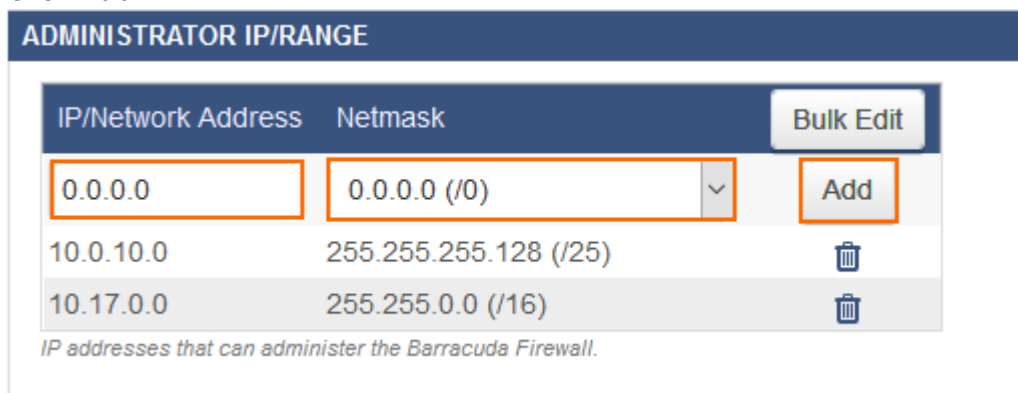
If administrators always use the same IP range, you can restrict access to the web interface of the firewall by specifying a range of allowed IP addresses or networks to increase security.

Misconfigurations of the administrator IP/range may cause the management web interface of the firewall to be unreachable. Contact Barracuda Networks Technical Support to recover connectivity.

1. Go to **BASIC > Administration**.
2. In the **ADMINISTRATOR IP/RANGE** section, enter the **IP/Network Address** and **Netmask** for the networks allowed to access the web interface. For a single IP address, set the **Netmask**

field to **255.255.255.255**.

3. Click **Add**.



IP/Network Address	Netmask	
0.0.0.0	0.0.0.0 (/0)	Add
10.0.10.0	255.255.255.128 (/25)	🗑️
10.17.0.0	255.255.0.0 (/16)	🗑️

IP addresses that can administer the Barracuda Firewall.

Step 3. (Optional) Additional configuration steps

You may need to complete the following tasks to finish the basic setup for your firewall:

- If needed, configure additional WAN connections. For more information, see [How to Configure WAN Interfaces](#).
- If you are using VLANs, configure the virtual interfaces. For more information, see [How to Configure a VLAN](#).
- Configure free ports for other networks. For more information, see [How to Configure Static Network Interfaces](#).

Step 4. Explore the Barracuda NextGen Firewall X-Series

After setting up the firewall, explore the following areas to learn where to get necessary information when working with your firewall and its services:

Subscription Status

To verify the status of your licenses, go to the **BASIC > Status** page and view the **Subscription Status** section. The status for all purchased licenses displays as **Current**. While the firewall is connected to the Internet, it automatically downloads licenses. If the firewall cannot be activated, please contact [Barracuda Networks Technical Support](#).

Firmware Update

To verify that the firewall is using the latest available firmware, go to the **ADVANCED > Firmware Update** page. For production, use the latest general release firmware version. Before updating the appliance, read the release notes for information on new features, bug fixes, and possible migration

instructions.

Network

To view the status of the following:

- **Network routes and interfaces** – Go to the **NETWORK > Routing** page.
- **Network interface links** – Go to the **BASIC > Status** page and move the mouse over the ports displayed in the **Link Status** section.

To view the configurations:

- **Network interfaces** – Go to the **NETWORK > IP Configuration** page and view the **Network Interface Configuration** section.
- **Bridges** – Go to the **NETWORK > Bridging** page. Before you deploy the firewall for use in production, delete the port 1—port 3 bridge.

For more information on networking, see [Networking](#).

Firewall

To view access rules, go to the **FIREWALL > Firewall Rules** page.

To monitor currently active and recently established and completed connections, go to the following pages:

- **BASIC > Active Connections**
- **BASIC > Recent Connections**

For more information on the firewall and firewall rules, see [Firewall](#).

Next steps

After setting up and exploring the firewall, you can complete the following tasks:

- Connect the firewall to your existing authentication service or create a built-in database for user information. For more information, see [Managing Users and Groups](#).
- If supported by your firewall model, configure Wi-Fi. For more information, see [How to Configure Wi-Fi](#).
- Configure site-to-site VPN. For more information, see [Site-to-Site VPN](#).
- Configure client-to-site VPN access. For more information, see [Client-to-Site VPN](#)
- Link the firewall with your Barracuda Cloud Control account for central management and

configuration. For more information, see [How to Connect to Barracuda Cloud Control](#)

- Configure the Barracuda Web Security Service, a cloud-based web filtering and security service. For more information, see [How to Configure the Barracuda Web Security Service](#)
- Set up an authoritative DNS. For more information, see [Authoritative and Caching DNS](#).
- Configure a DMZ. For more information, see [How to Configure a DMZ](#)

Figures

1. acl.png

© 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.