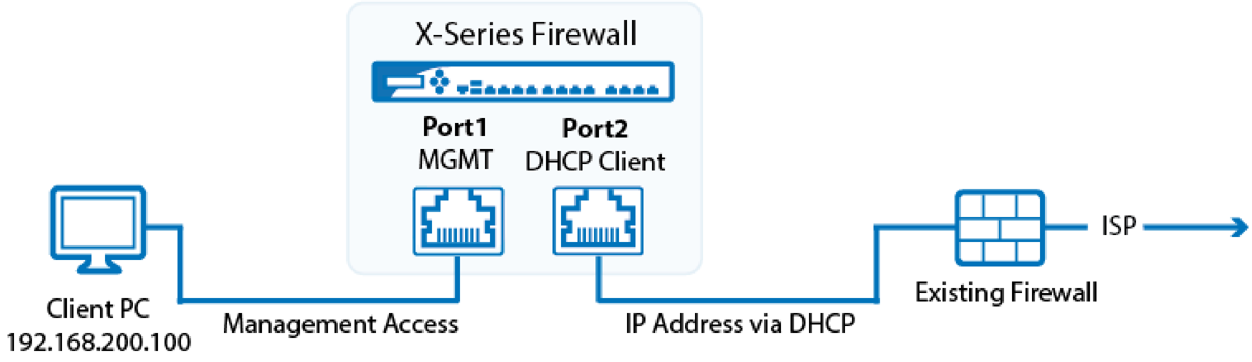
Getting Started

https://campus.barracuda.com/doc/8650767/

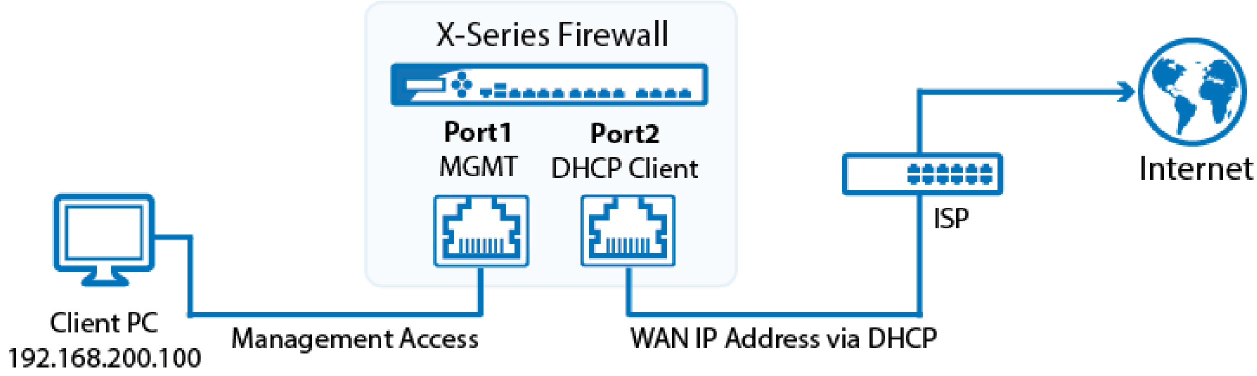
> These instructions are an expanded version of the Barracuda NextGen Firewall X-Series Quick Start Guide that was shipped with your appliance. If you have already completed the steps in the Quick Start Guide, go to Step 4.

To get started with your Barracuda NextGen Firewall X-Series, you must complete the activation procedure and integrate the firewall into your existing network. You can also directly replace an existing firewall if your ISP assigns the WAN IP address via DHCP. For all other types of Internet connections, you must first complete activation and basic setup in the existing network. After completing the basic setup wizard, you can evaluate the X-Series Firewall as a firewall, using one of the firewall configuration wizards, or as a remote access gateway, using the Remote Access Gateway wizard.

Barracuda NextGen Firewall X-Series in an Existing Network



Barracuda NextGen Firewall X-Series directly Attached to a DHCP ISP Connection



Before You Begin

Unpack the NextGen X-Series Firewall and verify that you have all of the following accessories:

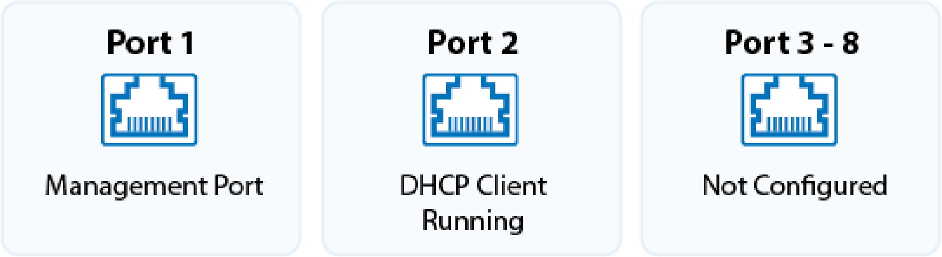
- Barracuda NextGen X-Series Firewall (verify that you have received the correct model)
- AC power cord
- Power supply (X100/X101/X200/X201 only)
- Wi-Fi antenna (X101/X201 only)
- Mounting brackets (X300 and above)
- Ethernet cable

If any items are missing or damaged, contact your Barracuda sales representative.

Step 1. Connect Your PC to the NextGen X-Series Firewall

The number of ports depends on your model. By default, the ports are configured as follows:

- **Port 1**: Management port (access to the management interface)
- **Port 2**: DHCP client
- **Port 3-8**: Not configured



1. Plug in your client PC to **Port 1** of the firewall.
2. Plug in your Internet connection to **Port 2** of the firewall.

The X-Series Firewall must be assigned an IP address by a DHCP server in your network or a DHCP server of your ISP.

Step 2. Set a Static IP Address on the Client PC

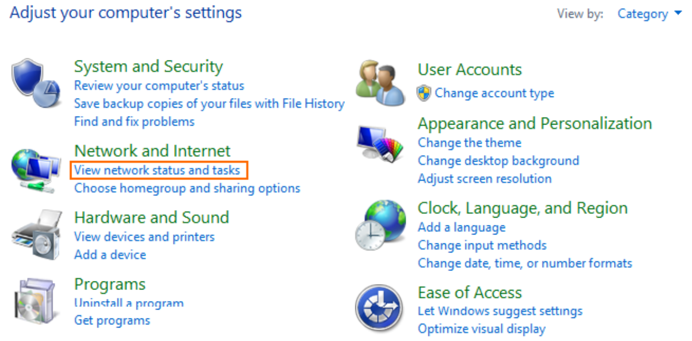
Configure your client PC to use the following static IP address configuration for the network interface connected to the firewall:

- **IP Address** – 192.168.200.100
- **Netmask** – 255.255.255.0
- **Gateway** – 192.168.200.200
- **DNS Servers** – Enter DNS servers in your network, or use public DNS servers such as the Google DNS servers 8.8.8.8 and 8.8.4.4.

Windows 8 / 8.1

You must have administrative rights to set the IP address on Microsoft Windows 8 / 8.1.

1. Open the **Control Panel** and click **View network status and tasks**. The **Network and Sharing Center** window opens.



Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
Save backup copies of your files with File History
Find and fix problems

Network and Internet
View network status and tasks
Choose homegroup and sharing options

Hardware and Sound
View devices and printers
Add a device

Programs
Uninstall a program
Get programs

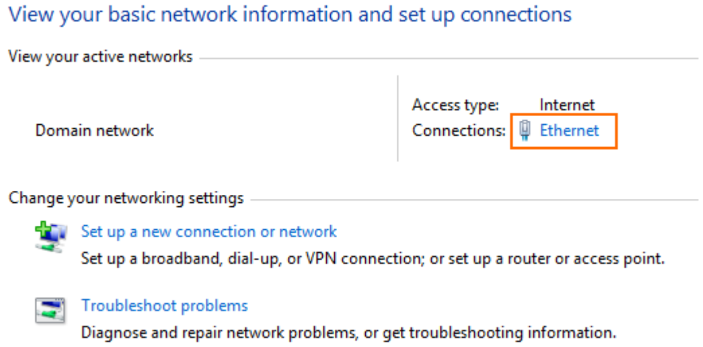
User Accounts
Change account type

Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution

Clock, Language, and Region
Add a language
Change input methods
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

2. In the **View your active networks** list, click on the name of the network interface connected to the firewall. For example, if you click on **Ethernet**, the **Ethernet Status** window opens.



View your basic network information and set up connections

View your active networks

Domain network

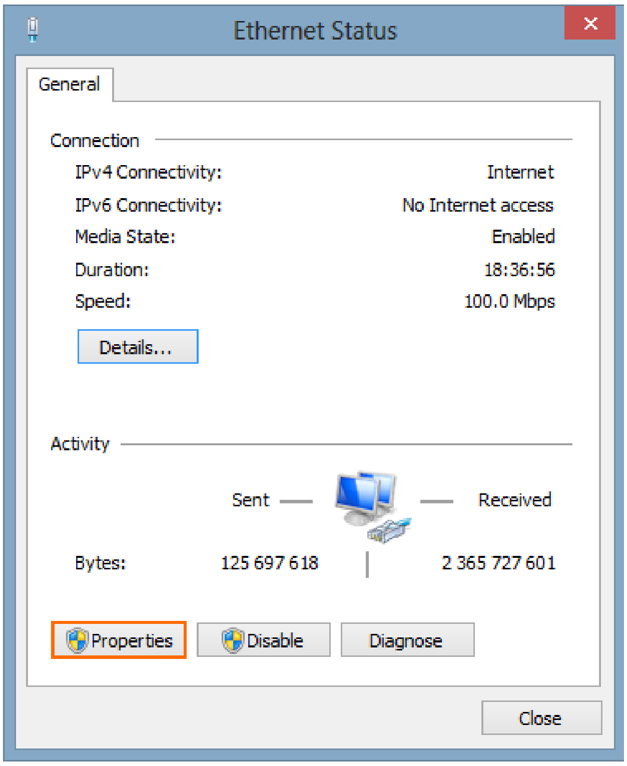
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

3. Click **Properties** and double-click on **Internet Protocol Version 4 (TCP/IPv4)**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** windows opens.



Ethernet Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No Internet access

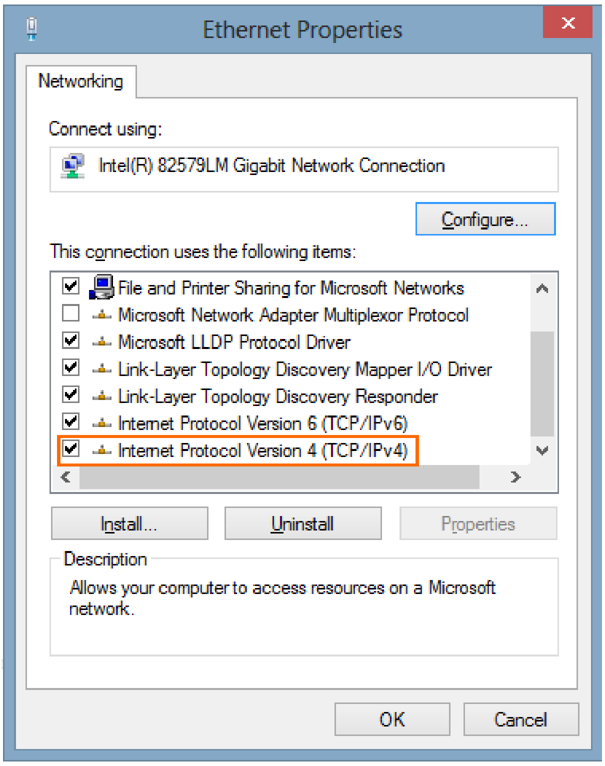
Media State: Enabled

Duration: 18:36:56

Speed: 100.0 Mbps

Activity

	Sent	Received
Bytes:	125 697 618	2 365 727 601



Ethernet Properties

Networking

Connect using:

Intel(R) 82579LM Gigabit Network Connection

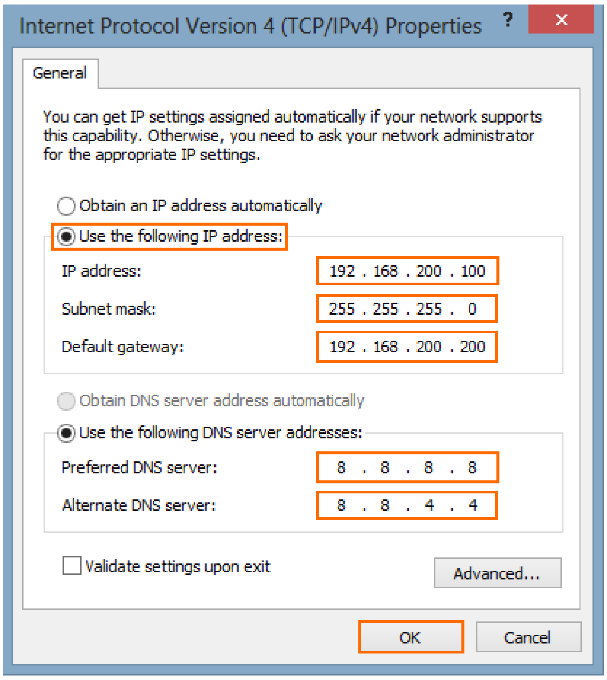
This connection uses the following items:

- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Allows your computer to access resources on a Microsoft network.

4. Select **Use the following IP address:.** Enter the static IP address, netmask, default gateway, and DNS servers.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 200 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 200 . 200

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: 8 . 8 . 4 . 4

☐ Validate settings upon exit

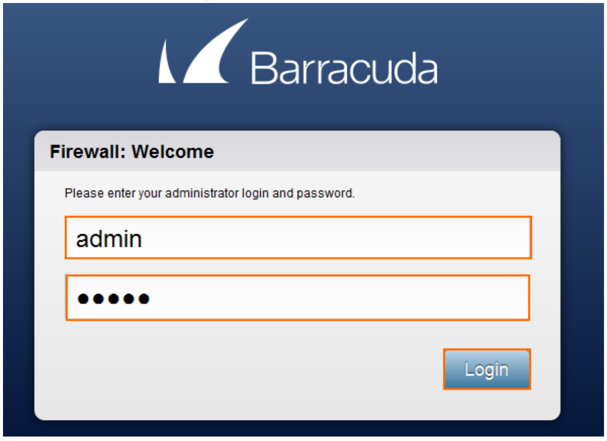
5. Click **OK**.

You are now using a static IP address.

Step 3. Log into the Web Interface

Access the web interface of the X-Series Firewall.

1. Go to https://192.168.200.200 in your browser.
2. Proceed at the certificate warning.
3. Log into the web interface with the default user credentials:
    - **Default username** – admin
    - **Default password** – admin



Firewall: Welcome

Please enter your administrator login and password.

admin

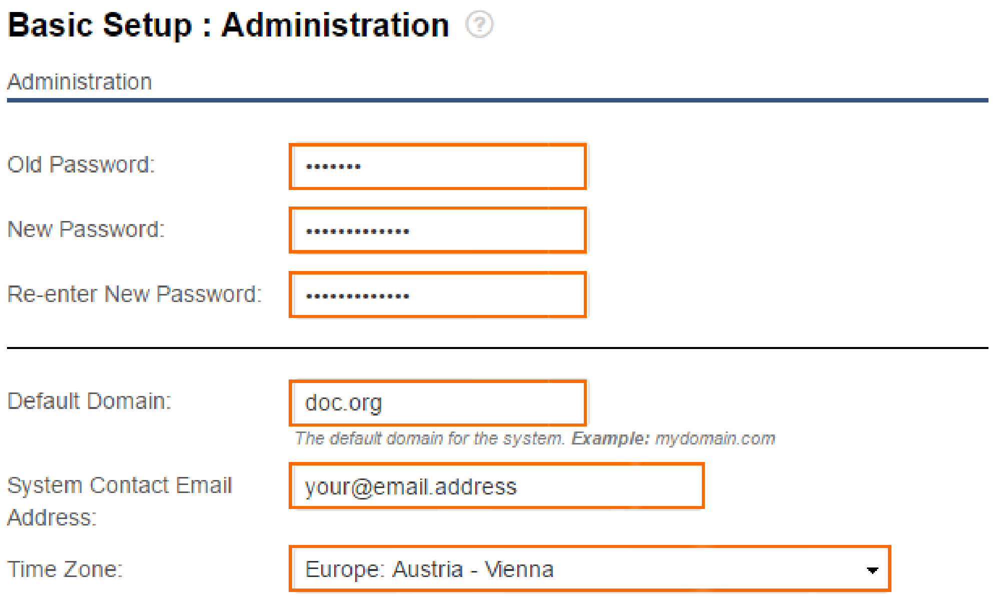
●●●●●

4. The **Basic Setup** wizard automatically launches.

Step 4. Complete the Basic Setup Wizard

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

1. Change the **Password**: The default password is **admin**.
2. Enter the default domain for your network.
3. Enter the **System Contact Email Address**. You will receive emails from Barracuda Central at this email address.
4. Select the **Time Zone**.



Basic Setup : Administration

Administration

Old Password: •••••••

New Password: •••••••••••••

Re-enter New Password: •••••••••••••

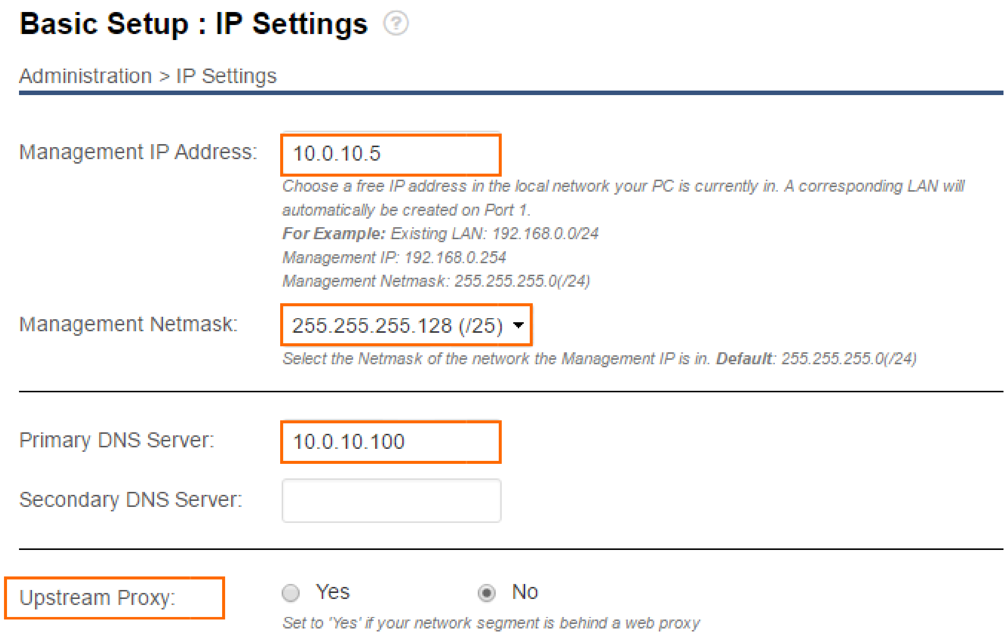
Default Domain: doc.org

*The default domain for the system. **Example:** mydomain.com*

System Contact Email Address: your@email.address

Time Zone: Europe: Austria - Vienna

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



Basic Setup : IP Settings

Administration > IP Settings

Management IP Address: 10.0.10.5

Choose a free IP address in the local network your PC is currently in. A corresponding LAN will automatically be created on Port 1.
***For Example:** Existing LAN: 192.168.0.0/24*
Management IP: 192.168.0.254
Management Netmask: 255.255.255.0(/24)

Management Netmask: 255.255.255.128 (/25)

*Select the Netmask of the network the Management IP is in. **Default:** 255.255.255.0(/24)*

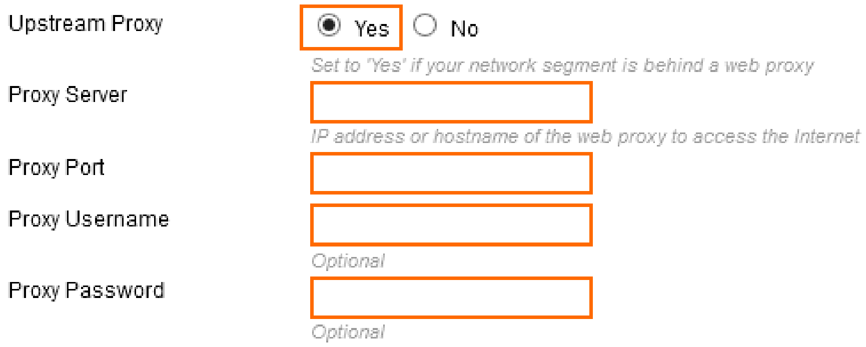
Primary DNS Server: 10.0.10.100

Secondary DNS Server:

Upstream Proxy: ○ Yes ● No

Set to 'Yes' if your network segment is behind a web proxy

9. (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.



Upstream Proxy ● Yes ○ No
Set to 'Yes' if your network segment is behind a web proxy

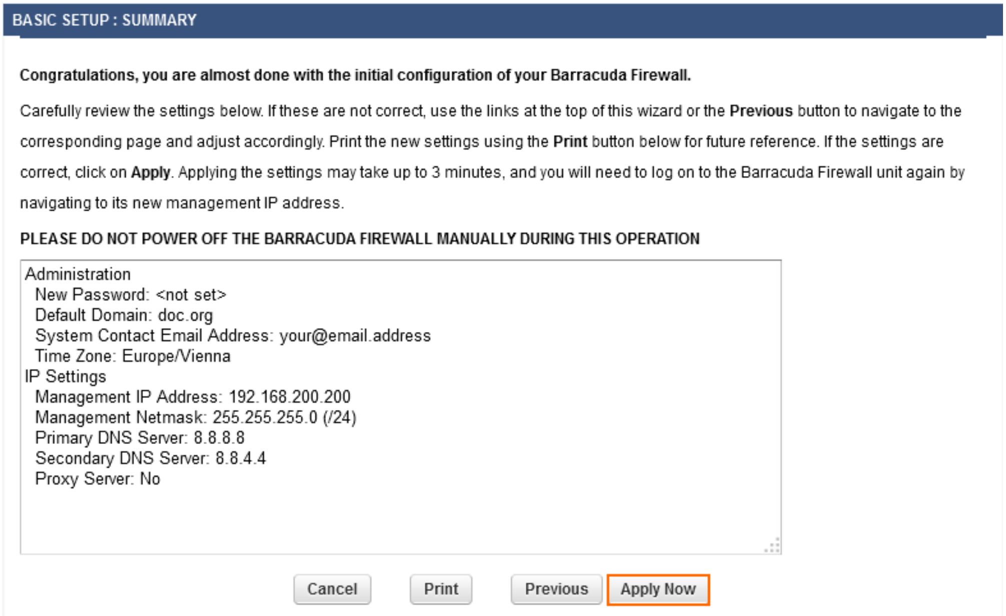
Proxy Server
IP address or hostname of the web proxy to access the Internet

Proxy Port

Proxy Username
Optional

Proxy Password
Optional

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



BASIC SETUP : SUMMARY

Congratulations, you are almost done with the initial configuration of your Barracuda Firewall.

Carefully review the settings below. If these are not correct, use the links at the top of this wizard or the **Previous** button to navigate to the corresponding page and adjust accordingly. Print the new settings using the **Print** button below for future reference. If the settings are correct, click on **Apply**. Applying the settings may take up to 3 minutes, and you will need to log on to the Barracuda Firewall unit again by navigating to its new management IP address.

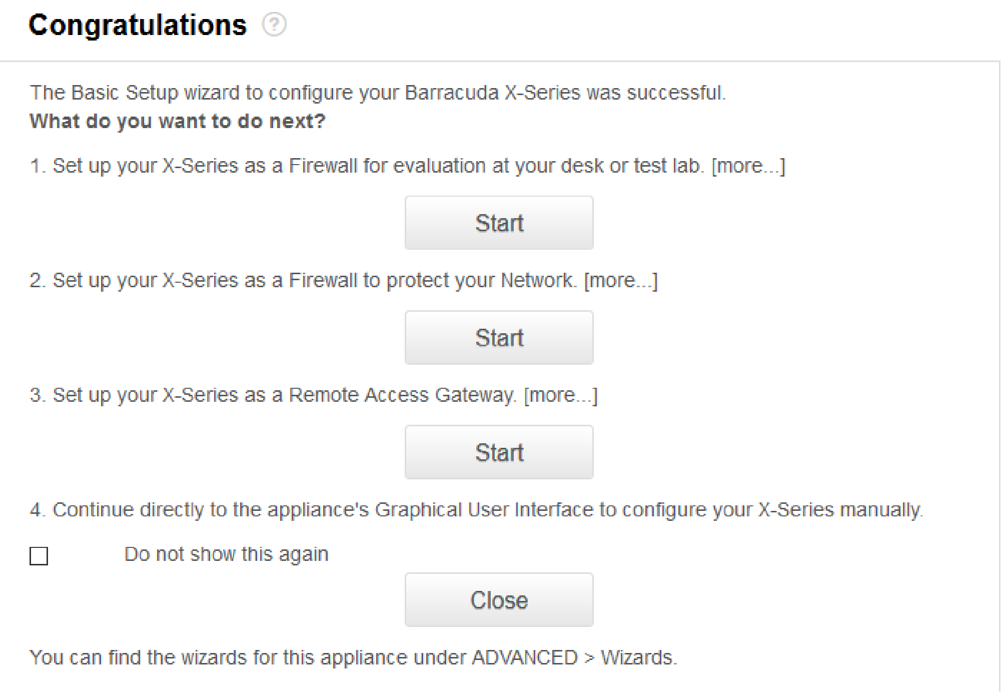
PLEASE DO NOT POWER OFF THE BARRACUDA FIREWALL MANUALLY DURING THIS OPERATION

```
Administration
  New Password: <not set>
  Default Domain: doc.org
  System Contact Email Address: your@email.address
  Time Zone: Europe/Vienna
IP Settings
  Management IP Address: 192.168.200.200
  Management Netmask: 255.255.255.0 (/24)
  Primary DNS Server: 8.8.8.8
  Secondary DNS Server: 8.8.4.4
  Proxy Server: No
```

If you changed the time zone, the X-Series Firewall will now reboot.

Next Steps

After the reboot, select a wizard for a customized setup, or configure the appliance manually:



Congratulations

The Basic Setup wizard to configure your Barracuda X-Series was successful.
What do you want to do next?

1. Set up your X-Series as a Firewall for evaluation at your desk or test lab. [more...]

2. Set up your X-Series as a Firewall to protect your Network. [more...]

3. Set up your X-Series as a Remote Access Gateway. [more...]

4. Continue directly to the appliance's Graphical User Interface to configure your X-Series manually.

□ Do not show this again

You can find the wizards for this appliance under ADVANCED > Wizards.

- As a firewall, by completing the configuration wizard matching your use case. For more information, see Deploy as Firewall.
- As a remote access gateway 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