CONTENTS

1 Out of the Box 2
2 How-To Guides 33
3 References 40
This Quick Start Guide covers the first time connection procedures for the Netgate® XG-1537 1U Firewall Appliance and will provide the information needed to keep the appliance up and running.

Tip: Before getting started, we recommend downloading the PDF version of the Product Manual and the PDF version of the pfSense Documentation in case you lose Internet access.
1.1 Getting Started

The basic firewall configuration begins with connecting the Netgate® appliance to the Internet. Neither the modem nor the Netgate appliance should be powered on at this time.

Establishing a connection to an Internet Service Provider (ISP) starts with connecting one end of an Ethernet cable to the WAN port (shown in the *Input and Output Ports* section) of the Netgate appliance.

**Warning:** The default LAN subnet on the firewall is 192.168.1.0/24. The same subnet cannot be used on both WAN and LAN, so if the subnet on the WAN side of the firewall is also 192.168.1.0/24, disconnect the WAN interface until the LAN interface has been renumbered to a different subnet.

The opposite end of the same Ethernet cable should be inserted into the LAN port of the ISP-supplied modem. The modem provided by the ISP might have multiple LAN ports. If so, they are usually numbered. For the purpose of this installation, please select port 1.

The next step is to connect the LAN port (shown in the *Input and Output Ports* section) of the Netgate appliance to the computer which will be used to access the firewall console. Connect one end of the second Ethernet cable to the LAN port (shown in the *Input and Output Ports* section) of the Netgate appliance. Connect the other end to the network connection on the computer. In order to access the webConfigurator, the PC network interface must be set to use DHCP, or have a static IP set in the 192.168.1.x subnet with a subnet mask of 255.255.255.0. Do not use 192.168.1.1, as this is the address of the firewall, and will cause an IP conflict.

1.1.1 Initial Setup

The next step is to power up the modem and the firewall. Plug in the power supply to the power port (shown in the *Input and Output Ports* section).

Once the modem and Netgate appliance are powered up, the next step is to power up the computer.

Once the Netgate appliance is booted, the attached computer should receive a 192.168.1.x IP address via DHCP from the Netgate appliance.
1.1.2 Logging Into the Web Interface

Browse to https://192.168.1.1 to access the web interface. In some instances, the browser may respond with a message indicating a problem with website security. Below is a typical example in Google Chrome. If this message or similar message is encountered, it is safe to proceed.

At the login page enter the default password and username:

- **Username**: admin
- **Password**: pfsense

Click **Login** to continue.
1.1.3 Wizard

Upon successful login, the following is displayed.

1.1.4 Configuring Hostname, Domain Name and DNS Servers

1.1.5 Hostname

For **Hostname**, any desired name can be entered as it does not affect functionality of the firewall. Assigning a hostname to the firewall will allow the GUI to be accessed by hostname as well as IP address.

For the purposes of this guide, use **pfsense** for the hostname. The default hostname, **pfsense** may be left unchanged.

Once saved in the configuration, the GUI may be accessed by entering http://pfsense as well as http://192.168.1.1

1.1.6 Domain

If an existing DNS domain is in use within the local network (such as a Microsoft Active Directory domain), use that domain here. This is the domain suffix assigned to DHCP clients, which should match the internal network.

For networks without any internal DNS domains, enter any desired domain name. The default **localdomain** is used for the purposes of this tutorial.
1.1.7 DNS Servers

The DNS server fields can be left blank if the DNS Resolver is used in non-forwarding mode, which is the default behavior. The settings may also be left blank if the WAN connection is using DHCP, PPTP or PPPoE types of Internet connections and the ISP automatically assigns DNS server IP addresses. When using a static IP on WAN, DNS server IP addresses must be entered here for name resolution to function if the default DNS Resolver settings are not used.

DNS servers can be specified here even if they differ from the servers assigned by the ISP. Either enter the IP addresses provided by the ISP, or consider using Google public DNS servers (8.8.8.8, 8.8.4.4). Google DNS servers are used for the purpose of this tutorial. Click Next after filling in the fields as appropriate.

1.1.8 Time Server Configuration

1.1.9 Time Server Synchronization

Setting time server synchronization is quite simple. We recommend using the default time server address, which will randomly select an NTP server from a pool.

1.1.10 Setting Time Zone

Select an appropriate time zone for the location of the firewall. For purposes of this manual, the Timezone setting will be set to America/Chicago for US Central time.

1.1.11 Configuring Wide Area Network (WAN) Type

The WAN interface type is the next to be configured. The IP address assigned to this section becomes the Public IP address that this network will use to communicate with the Internet.
This depicts the four possible WAN interface types. Static, DHCP, PPPoE and PPTP. One must be selected from the drop-down list.

Further information from the ISP is required to proceed when selecting Static, PPPoE and PPTP such as login name and password or as with static addresses, an IP address, subnet mask and gateway address.

DHCP is the most common type of interface for home cable modems. One dynamic IP address is issued from the ISP DHCP server and will become the public IP address of the network behind this firewall. This address will change periodically at the discretion of the ISP. Select DHCP as shown and proceed to the next section.

1.1.12 MAC Address

If replacing an existing firewall, the WAN MAC address of the old firewall may be entered here, if it can be determined. This can help avoid issues involved in switching out firewalls, such as ARP caches, ISPs locking to single MAC addresses, etc.

If the MAC address of the old firewall cannot be located, the impact is most likely insignificant. Power cycle the ISP router and modem and the new MAC address will usually be able to get online. For some ISPs, it may be necessary to call them when switching devices, or an activation process may be required.

1.1.13 Configuring MTU and MSS

MTU or Maximum Transmission Unit determines the largest protocol data unit that can be passed onwards. A 1500-byte packet is the largest packet size allowed by Ethernet at the network layer and for the most part, the Internet so leaving this field blank allows the system to default to 1500-byte packets. PPPoE is slightly smaller at 1492-bytes. Leave this blank for a basic configuration.
1.1.14 Configuring DHCP Hostname

Some ISPs specifically require a DHCP Hostname entry. Unless the ISP requires the setting, leave it blank.

1.1.15 Configuring PPPoE and PPTP Interfaces

Information added in these sections is assigned by the ISP. Configure these settings as directed by the ISP.
1.1.16 Block Private Networks and Bogons

When enabled, all private network traffic originating on the internet is blocked. Private addresses are reserved for use on internal LANs and blocked from outside traffic so these address ranges may be reused by all private networks.

The following inbound address Ranges are blocked by this firewall rule:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.254
- 192.168.0.0 to 192.168.255.254
- 127.0.0.0/8
- 100.64.0.0/10
- fc00::/7

Bogons are public IP addresses that have not yet been allocated, so they may typically also be safely blocked as they should not be in active use.

Check Block RFC1918 Private Networks and Block Bogon Networks.

Click Next to continue.

1.1.17 Configuring LAN IP Address & Subnet Mask

On this screen the Local Area Network information will be configured.

<table>
<thead>
<tr>
<th>LAN IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>24</td>
</tr>
</tbody>
</table>

Click Next to continue.
A static IP address of 192.168.1.1 and a subnet mask (CIDR) of 24 was chosen for this installation. If there are no plans to connect this network to any other network via VPN, the 192.168.1.x default is sufficient.

Click Next to continue.

**Note:** If a Virtual Private Network (VPN) is configured to remote locations, choose a private IP address range more obscure than the very common 192.168.1.0/24. IP addresses within the 172.16.0.0/12 RFC1918 private address block are the least frequently used. We recommend selecting a block of addresses between 172.16.x.x and 172.31.x.x for least likelihood of having VPN connectivity difficulties. An example of a conflict would be If the local LAN is set to 192.168.1.x and a remote user is connected to a wireless hotspot using 192.168.1.x (very common), the remote client won’t be able to communicate across the VPN to the local network.

### 1.1.18 Change Administrator Password

In this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

<table>
<thead>
<tr>
<th>Admin Password</th>
<th>Admin Password AGAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>********</td>
<td></td>
</tr>
</tbody>
</table>

Select a new **Administrator Password** and enter it twice, then click Next to continue.

### 1.1.19 Save Changes

Click **Reload** to save configuration.
1.1.20 Basic Firewall Configured

To proceed to the webConfigurator, make the selection as highlighted. The Dashboard display will follow.

1.1.21 Backing Up and Restoring

At this point, basic LAN and WAN interface configuration is complete. Before proceeding, backup the firewall configuration. From the menu at the top of the page, browse to Diagnostics > Backup/Restore.
Click **Download Configuration** and save a copy of the firewall configuration.

This configuration can be restored from the same screen by choosing the backup file under **Restore configuration**.
1.1.22 Connecting to the Console

There are times when accessing the console is required. Perhaps GUI console access has been locked out, or the password has been lost or forgotten.

See also:

Connecting to the Console Port  Connect to the console. Cable is required.

Tip:  To learn more about getting the most out of your Netgate appliance, sign up for a pfSense Plus Training course or browse our extensive Resource Library.

1.2 Initial Configuration

Plug the power cable into the power port and press the power button on the front left (shown in the Input and Output Ports section) to turn on the Netgate® Firewall. Allow 4 or 5 minutes to boot up completely.

Warning:  If your DSL or Cable Modem has a default IP Address of 192.168.1.1, please disconnect the Ethernet cable from the WAN port on your XG-1537 1U Netgate Security Gateway before proceeding. You will need to change the default IP Address of the device during a later step in the configuration.

1. From the computer, log into the Web Interface

Open a web browser (Google Chrome in this example) and type in 192.168.1.1 on the address bar. Press Enter.

Fig. 1: Enter the Default LAN IP Address

2. A warning message may appear. If this message or similar message is encountered, it is safe to proceed. Click the Advanced Button and the click Proceed to 192.168.1.1 (unsafe) to continue.

3. At the Sign In page, enter the default pfSense® Plus username and password and click Next.
   • Default Username: admin
   • Default Password: pfsense
1.2.1 The Setup Wizard

The following steps will step through the Setup Wizard for the initial configuration of the firewall.

**Note:** Ignore the warning to reset the ‘admin’ account password. One of the steps in the Setup Wizard is to change the default password.

1. Click Next to start the Setup Wizard.
2. Click Next after you have read the information on Netgate Global Support.
3. On the General Information page, use the following as a guide to configure the firewall.
   - **Hostname:** Any desired name can be entered. For the purposes of this guide, the default hostname `pfsense` is used.
   - **Domain:** The default `localdomain` is used for the purposes of this tutorial.
   - **DNS Servers:** For purposes of this setup guide, use the Google public DNS servers (8.8.8.8 and 8.8.4.4).
4. Use the following information for the Time Server Information page.
   - **Time Server Hostname:** Use the default time server address.
   - **Timezone:** Select the time zone for the location of the firewall. For this guide, the Timezone will be set to America/Chicago for US Central time.
5. The WAN interface is the Public IP address the network will use to communicate with the Internet. Use the following information for the WAN configuration page.
   - **DHCP** is the default and is the most common type of interface for home cable modems.
   - **Default settings** for the other items on this page should be acceptable for normal home users.
Fig. 3: Click Next

Fig. 4: Type in the DNS Server information and Click Next
Fig. 5: Change the Timezone and Click Next

Fig. 6: Default Settings Should Be Acceptable. Click Next
6. Configuring LAN IP Address & Subnet Mask. The default LAN IP address of 192.168.1.1 and subnet mask of 24 is usually sufficient.

**Tip:** If your DSL or Cable Modem has a default IP Address of 192.168.1.1, change the IP Address of your XG-1537 1U Netgate Security Gateway to a different subnet, such as 192.168.2.1 with a subnet mask of 24 to avoid an IP Address conflict.

7. Change the Admin Password. Enter the same password in both fields.

8. Click Reload to save the configuration.

9. After a few seconds, a message will indicate the Setup Wizard has completed. To proceed to the pfSense® Plus dashboard, click Finish.

10. A final notification screen will appear with the Copyright and Trademark Notices. Read and click Accept to continue to the dashboard.

---

**Copyright and Trademark Notices.**

Copyright © 2004-2016, Electric Sheep Fencing, LLC (“ESF”). All Rights Reserved.
Copyright © 2014-2021, Rubicon Communications, LLC d/b/a Netgate (“Netgate”). All Rights Reserved.

All logos, text and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.

pfSense® software is open source and distributed under the Apache 2.0 license. However, no commercial distribution of ESF and/or Netgate software is allowed without the prior written consent of ESF and/or Netgate.

ESF and/or Netgate make no warranty of any kind, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. ESF and/or Netgate shall not be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of any software, information, or material.

**Restricted Rights Legend.**

No part of ESF and/or Netgate’s information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.

Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

**Regulatory/Export Compliance.**

The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government’s Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.
If you unplugged the Ethernet cable at the beginning of this configuration, reconnect it to the WAN port now. This completes the basic configuration for the Netgate appliance.

1.3 pfSense Plus Overview

This page provides an overview of the pfSense® Plus dashboard and navigation. It also provides information on how to perform frequent tasks such as backing up the pfSense® Plus software and connecting to the Netgate firewall console.

1.3.1 The Dashboard

pfSense® Plus software is highly configurable, all of which can be done through the dashboard. This orientation will help to navigate and further configure the firewall.

![The pfSense® Plus Dashboard](image)

Fig. 8: The pfSense® Plus Dashboard

**Section 1** shows important system information such as the model, Serial Number, and Netgate Device ID for this Netgate firewall.

**Section 2** identifies what version of pfSense® Plus software is installed, and if an update is available.

**Section 3** describes Netgate Service and Support.

**Section 4** shows the various menu headings. Each menu heading has drop-down options for a wide range of configuration choices.
1.3.2 Re-running the Setup Wizard

To re-run the Setup Wizard, navigate to System -> Setup Wizard.

![Setup Wizard](image)

Fig. 9: Re-run the Setup Wizard

1.3.3 Backup and Restore

It is important to backup the firewall configuration prior to updating or making any configuration changes. From the menu at the top of the page, browse to Diagnostics > Backup/Restore.

Click Download configuration as XML and save a copy of the firewall configuration to the computer connected to the Netgate firewall.

This backup (or any backup) can be restored from the same screen by choosing the backed up file under Restore Configuration.

**Note:** Auto Config Backup is a built-in service located at Services -> Auto Config Backup. This service will save up to 100 encrypted backup files automatically, any time a change to the configuration has been made. Visit the Auto Config Backup page for more information.
Fig. 10: Backup & Restore

Fig. 11: Click Download configuration as XML
Connecting to the Console

There are times when accessing the console is required. Perhaps GUI console access has been locked out, or the password has been lost or forgotten.

See also:

*Connecting to the Console Port* Connect to the console. Cable is required.

Tip: To learn more about getting the most out of your Netgate appliance, sign up for a pfSense Plus Training course or browse our extensive Resource Library.

1.4 Input and Output Ports

1.4.1 Front Side

![Front Side Diagram]

Network Ports

Default Ports

When no expansion card is installed, this is the port configuration.

<table>
<thead>
<tr>
<th>Port</th>
<th>Interface Name</th>
<th>Port Name</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>WAN</td>
<td>igb0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>1</td>
<td>LAN</td>
<td>igb1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>OPT1</td>
<td>ix0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>OPT2</td>
<td>ix1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

Note: Both the WAN and LAN ports of the Netgate® appliance support auto-MDIX and are capable of utilizing either straight-through or crossover ethernet cables.

Warning: The ix(4) driver used for ports IX0-IX1 does not support ALTQ traffic shaping directly. Limiters may be used instead, or use tagged VLAN interfaces which can be used with ALTQ traffic shaping.
Optional Intel 1 Gbps Expansion Card Ports

When the 4 port Intel 1 Gbps Ethernet Expansion Card is installed, this is the port configuration.

<table>
<thead>
<tr>
<th>Port</th>
<th>Interface Name</th>
<th>Port Name</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OPT6</td>
<td>igb0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>1</td>
<td>OPT5</td>
<td>igb1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>OPT4</td>
<td>igb2</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>OPT3</td>
<td>igb3</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>WAN</td>
<td>igb4</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>LAN</td>
<td>igb5</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>6</td>
<td>OPT1</td>
<td>ix0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>7</td>
<td>OPT2</td>
<td>ix1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

Optional Chelsio 10 Gbps Expansion Card Ports

When the 2 port Chelsio 10 Gbps Ethernet Expansion Card is installed, this is the port configuration.

<table>
<thead>
<tr>
<th>Port</th>
<th>Interface Name</th>
<th>Port Name</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>WAN</td>
<td>cxl0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>1</td>
<td>LAN</td>
<td>cxl1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>OPT1</td>
<td>igb0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>OPT3</td>
<td>igb1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>OPT2</td>
<td>ix0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>OPT4</td>
<td>ix1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>
Network Port LEDs

Both the RJ-45 and SFP+ Network Ports have LEDs indicating status.

RJ-45 Ports

Table 1: RJ-45 LEDs Configuration

<table>
<thead>
<tr>
<th>Activity LED (Left)</th>
<th>Link Speed LED (Right)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off = No Connection</td>
<td>Amber = 1 Gbps</td>
</tr>
<tr>
<td>Yellow Flashing = Activity</td>
<td>Green = 100 Mbps</td>
</tr>
<tr>
<td></td>
<td>Off = No Connection or 10 Mbps</td>
</tr>
</tbody>
</table>

Note: Reverse the above table for the bottom port as it is inverted.

SFP+ Ports

Table 2: SFP+ LEDs Configuration

<table>
<thead>
<tr>
<th>Left Two LEDs</th>
<th>Right Two LEDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off = No Connection</td>
<td>Green Blinking = Activity</td>
</tr>
<tr>
<td>Green = Connection Established</td>
<td></td>
</tr>
</tbody>
</table>

Note: The triangles point either up or down, indicating the port it is referring to.
Status LEDs

8
7

a b c d e
<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8a</td>
<td>Continuously on and red</td>
<td>An overheat condition has occurred. (This may be caused by cable congestion.)</td>
</tr>
<tr>
<td></td>
<td>Blinking red (1Hz)</td>
<td>Fan failure, check for an inoperative fan.</td>
</tr>
<tr>
<td></td>
<td>Blinking red (0.25Hz)</td>
<td>Power failure, check for a non-operational power supply.</td>
</tr>
<tr>
<td></td>
<td>Solid blue</td>
<td>Local UID has been activated. Use this function through IPMI to locate the server in a rack mount environment.</td>
</tr>
<tr>
<td></td>
<td>Blinking blue</td>
<td>Remote UID is on. Use this function through IPMI to identify the server from a remote location.</td>
</tr>
<tr>
<td>8b</td>
<td>Flashing</td>
<td>Indicates network activity on igb1 (upper left port).</td>
</tr>
<tr>
<td>8c</td>
<td>Flashing</td>
<td>Indicates network activity on igb0 (lower left port).</td>
</tr>
<tr>
<td>8d</td>
<td>Flashing</td>
<td>Indicates IDE channel activity on the hard drive.</td>
</tr>
<tr>
<td>8e</td>
<td>Illuminated</td>
<td>Indicates power is being supplied to the system power supply units. This LED should normally be illuminated when the system is operating.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Indicates no power is being supplied to the system power supply. System is powered off.</td>
</tr>
</tbody>
</table>
Other Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>I/O Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>IPMI</td>
</tr>
<tr>
<td>5</td>
<td>2x USB 3.0</td>
</tr>
<tr>
<td>6</td>
<td>VGA</td>
</tr>
<tr>
<td>7</td>
<td>Reset &amp; Power buttons</td>
</tr>
<tr>
<td>8</td>
<td>Status LEDs</td>
</tr>
</tbody>
</table>

1.4.2 Rear Side

Other Ports

1. Power port
   • Power Consumption 20W (idle)

1.5 Safety and Legal

1.5.1 Safety Notices

1. Read, follow, and keep these instructions.
2. Heed all warnings.
3. Only use attachments/accessories specified by the manufacturer.

**Warning:** Do not use this product in location that can be submerged by water.

**Warning:** Do not use this product during an electrical storm to avoid electrical shock.

1.5.2 Electrical Safety Information

1. Compliance is required with respect to voltage, frequency, and current requirements indicated on the manufacturer’s label. Connection to a different power source than those specified may result in improper operation, damage to the equipment or pose a fire hazard if the limitations are not followed.
2. There are no operator serviceable parts inside this equipment. Service should be provided only by a qualified service technician.
3. This equipment is provided with a detachable power cord which has an integral safety ground wire intended for connection to a grounded safety outlet.
   a) Do not substitute the power cord with one that is not the provided approved type. If a 3 prong plug is provided, never use an adapter plug to connect to a 2-wire outlet as this will defeat the continuity of the grounding wire.
   b) The equipment requires the use of the ground wire as a part of the safety certification, modification or misuse can provide a shock hazard that can result in serious injury or death.
c) Contact a qualified electrician or the manufacturer if there are questions about the installation prior to connecting the equipment.

d) Protective grounding/earthing is provided by Listed AC adapter. Building installation shall provide appropriate short-circuit backup protection.

e) Protective bonding must be installed in accordance with local national wiring rules and regulations.

1.5.3 FCC Compliance

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and

2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment.

1.5.4 Industry Canada

This Class B digital apparatus complies with Canadian ICES-3(B). Cet appareil numérique de la classe B est conforme à la norme NMB-3(B) Canada.

1.5.5 Australia and New Zealand

This is a AMC Compliance level 2 product. This product is suitable for domestic environments.

1.5.6 CE Marking

CE marking on this product represents the product is in compliance with all directives that are applicable to it.

1.5.7 RoHS/WEEE Compliance Statement

English

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Español

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Français

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L’élimination et le recyclage en bonne et due forme ont pour but de lutter contre l’impact néfaste potentiel de ce type de produits sur l’environnement et la santé publique. Pour plus d’informations sur le mode d’élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l’endroit où vous avez acheté le produit.

Italiano

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull’imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l’ambiente e per la salute dell’essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.
1.5.8 Declaration of Conformity

Česky [Czech]

NETGATE tímto prohlašuje, e tento NETGATE device, je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.

Dansk [Danish]

Undertegnede NETGATE erklærer herved, at følgende udstyr NETGATE device, overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.

Nederlands [Dutch]

Hierbij verklaart NETGATE dat het toestel NETGATE device, in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze verklaart NETGATE dat deze NETGATE device, voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.

English

Hereby, NETGATE, declares that this NETGATE device, is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Eesti [Estonian]

Käesolevaga kinnitab NETGATE seadme NETGATE device, vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

Suomi [Finnish]

NETGATE vakuuttaa täten että NETGATE device, tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. Français [French] Par la présente NETGATE déclare que l’appareil Netgate, device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Deutsch [German]

Hiermit erklärt Netgate, dass sich diese NETGATE device, in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet”. (BMWi)
Ελληνικά [Greek]

ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGATE ΔΗΛΩΝΕΙ ΟΤΙ NETGATE device, ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1995/5/EK.

Magyar [Hungarian]

Alulírott, NETGATE nyilatkozom, hogy a NETGATE device, megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.

Íslenska [Icelandic]

Hér me l sir NETGATE yfir ví a NETGATE device, er í samræmi vi grunnkröfur og a rar kröfur, sem ger ar eru í tilskipun 1999/5/EC.

Italiano [Italian]

Con la presente NETGATE dichiara che questo NETGATE device, è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Latviski [Latvian]

Ar o NETGATE deklar, ka NETGATE device, atbilst Direkt vas 1999/5/EK b tiskaj m pras b m un citiem ar to saist tajiem noteikumiem.

Lietuviškai [Lithuanian]

NETGATE deklaruoja, kad šis NETGATE ı ˛renginys atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Malti [Maltese]

Hawnhekk, Netgate, jiddikjara li dan NETGATE device, jikkonforma mal- ti ijiet essenzjali u ma provvedimenti o rajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

Norsk [Norwegian]

NETGATE erklærer herved at utstyret NETGATE device, er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.
1.5.9 Disputes

ANY DISPUTE OR CLAIM RELATING IN ANY WAY TO YOUR USE OF ANY PRODUCTS/SERVICES, OR TO ANY PRODUCTS OR SERVICES SOLD OR DISTRIBUTED BY RCL OR ESF WILL BE RESOLVED BY BINDING ARBITRATION IN AUSTIN, TEXAS, RATHER THAN IN COURT. The Federal Arbitration Act and federal arbitration law apply to this agreement.

THERE IS NO JUDGE OR JURY IN ARBITRATION, AND COURT REVIEW OF AN ARBITRATION AWARD IS LIMITED. HOWEVER, AN ARBITRATOR CAN AWARD ON AN INDIVIDUAL BASIS THE SAME DAMAGES AND RELIEF AS A COURT (INCLUDING INJUNCTIVE AND DECLARATORY RELIEF OR STATUTORY DAMAGES), AND MUST FOLLOW THE TERMS OF THESE TERMS AND CONDITIONS OF USE AS A COURT WOULD.

To begin an arbitration proceeding, you must send a letter requesting arbitration and describing your claim to the following:

Rubicon Communications LLC
Attn.: Legal Dept.
4616 West Howard Lane, Suite 900
The arbitration will be conducted by the American Arbitration Association (AAA) under its rules. The AAA’s rules are available at www.adr.org. Payment of all filing, administration and arbitrator fees will be governed by the AAA’s rules.

We each agree that any dispute resolution proceedings will be conducted only on an individual basis and not in a class, consolidated or representative action. We also both agree that you or we may bring suit in court to enjoin infringement or other misuse of intellectual property rights.

1.5.10 Applicable Law

By using any Products/Services, you agree that the Federal Arbitration Act, applicable federal law, and the laws of the state of Texas, without regard to principles of conflict of laws, will govern these terms and conditions of use and any dispute of any sort that might arise between you and RCL and/or ESF. Any claim or cause of action concerning these terms and conditions or use of the RCL and/or ESF website must be brought within one (1) year after the claim or cause of action arises. Exclusive jurisdiction and venue for any dispute or claim arising out of or relating to the parties’ relationship, these terms and conditions, or the RCL and/or ESF website, shall be with the arbitrator and/or courts located in Austin, Texas. The judgment of the arbitrator may be enforced by the courts located in Austin, Texas, or any other court having jurisdiction over you.

1.5.11 Site Policies, Modification, and Severability

Please review our other policies, such as our pricing policy, posted on our websites. These policies also govern your use of Products/Services. We reserve the right to make changes to our site, policies, service terms, and these terms and conditions of use at any time.

1.5.12 Miscellaneous

If any provision of these terms and conditions of use, or our terms and conditions of sale, are held to be invalid, void or unenforceable, the invalid, void or unenforceable provision shall be modified to the minimum extent necessary in order to render it valid or enforceable and in keeping with the intent of these terms and conditions. If such modification is not possible, the invalid or unenforceable provision shall be severed, and the remaining terms and conditions shall be enforced as written. Headings are for reference purposes only and in no way define, limit, construe or describe the scope or extent of such section. Our failure to act with respect to a breach by you or others does not waive our right to act with respect to subsequent or similar breaches. These terms and conditions set forth the entire understanding and agreement between us with respect to the subject matter hereof, and supersede any prior oral or written agreement pertaining thereto, except as noted above with respect to any conflict between these terms and conditions and our reseller agreement, if the latter is applicable to you.
1.5.13 Limited Warranty

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

The products/services and all information, content, materials, products (including software) and other services included on or otherwise made available to you through the products/services are provided by us on an “as is” and “as available” basis, unless otherwise specified in writing. We make no representations or warranties of any kind, express or implied, as to the operation of the products/services, or the information, content, materials, products (including software) or other services included on or otherwise made available to you through the products/services, unless otherwise specified in writing. You expressly agree that your use of the products/services is at your sole risk.

To the full extent permissible by applicable law, Rubicon Communications, LLC (RCL) and Electric Sheep Fencing (ESF) disclaim all warranties, express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. RCL and ESF do not warrant that the products/services, information, content, materials, products (including software) or other services included on or otherwise made available to you through the products/services, RCL’s or ESF’s servers or electronic communications sent from RCL or ESF are free of viruses or other harmful components. RCL and ESF will not be liable for any damages of any kind arising from the use of any products/services, or from any information, content, materials, products (including software) or other services included on or otherwise made available to you through the products/services, including, but not limited to direct, indirect, incidental, punitive, and consequential damages, unless otherwise specified in writing.

In no event will RCL’s or ESF’s liability to you exceed the purchase price paid for the product or service that is the basis of the claim.

Certain state laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you, and you might have additional rights.
2.1 Connecting to the Console Port

Connecting to the VGA console is identical to connecting any computer to a monitor. Just connect the VGA cable (DB-15) between the Netgate® system and the monitor. Use USB or PS/2 keyboard and mouse as applicable to your hardware.

**Note:** If your system has both USB 2.0 (black) and USB 3.0 (blue) ports, use the USB 2.0 ports, as USB 3.0 is not supported in earlier versions of pfSense software.

**Note:** If your system has both VGA and serial, it is possible that the boot console will default to serial. If your boot process seems to hang after mounting the root volume, please see Boot Troubleshooting.

2.2 Accessing IPMI and Changing IPMI Password

**Note:** By default, the IPMI port is configured to be a DHCP client. When connected to a network with DHCP, the IP address will appear in the lower right corner of the screen during boot.

In compliance with new privacy legislation, the Username and Password to access the IPMI port on the Netgate XG-1537 1U has been changed to a unique password on each device. Netgate started shipping systems with this change beginning February 21, 2020.

Prior to February 21, 2020, the IPMI Username and Password were **ADMIN/ADMIN**.

After February 21, 2020, the IPMI Username is still **ADMIN**, the password is located on a sticker on the bottom of the XG-1537 as shown below.

**Note:** The password is alpha-numeric and the letters are capital letters.
Fig. 1: IPMI Password Sticker Location
2.2.1 Changing the IPMI Password

1. To change the IPMI password, begin by accessing the IPMI GUI using a web browser and the IPMI IP Address. Log in to the IPMI console.

![Log Into IPMI](image)

2. Navigate to Configuration -> Users.

3. Highlight the Administrator and click Modify User.

4. Check the box by Change Password, enter the new password and confirm it by typing it a second time, then click Modify.

5. Click OK on the message window that says “Modified user successfully.”

2.3 Reinstalling pfSense Plus Software

1. Please open a support ticket to request access to the factory firmware by selecting Firmware Access as the General Problem and then select Netgate XG-1537 1U for the platform. Make sure to include the serial number in the ticket to expedite access.

   Once the ticket is processed, the latest stable version of the firmware will be attached to the ticket, with a name such as:
   
   pfSense-plus-memstick-21.02-RELEASE-amd64.img.gz

   **Note:** pfSense® Plus is preinstalled on Netgate appliances, which is optimally tuned for our hardware and
Fig. 3: Configuration -> Users

Fig. 4: Modify User
Fig. 5: Change Password and click Modify

Fig. 6: Click OK
contains some features that cannot be found elsewhere, such as the AWS VPC Wizard.

2. Write the image to a USB memstick. Locating the image and writing it to a USB memstick is covered in detail under Writing Flash Drives.

3. Connect to the console port of the Netgate device.

4. Insert the memstick into an open USB port and boot the system.

5. After a minute the pfSense® Plus loader menu will be displayed with a 3 second timer. Either allow the menu to timeout or press 1 (the default) to continue.

6. Console options are presented for serial console installation. The default option is vt100, which should work for most. Choose the correct console output for your system.

![PFSense loader menu](image)

Please choose the appropriate terminal type for your system.

Common console types are:

- ansi Standard ANSI terminal
- vt100 VT100 or compatible terminal
- xterm xterm terminal emulator (or compatible)
- cons25w cons25w terminal

7. The installer will automatically launch and several options will be presented. On Netgate appliances, choosing Enter for the default options will complete the installation process.

Note: Options such as the type of disk partition can be modified through this installation if required.

8. Once the installer is finished, choose No and press Enter to skip going to a shell.

9. The installer will then prompt to Reboot the system. Select Reboot and press Enter. The system will shutdown and reboot.

Dec 21 22:41:37 Waiting (max 60 seconds) for system process `vniru` to stop... done

(continues on next page)
10. Remove the USB drive from the USB port.

**Important:** If the USB drive remains attached, the system will boot into the installer again because by default the system firmware is configured so that a device plugged into the USB port will be booted with a higher priority.

See also:

For information on restoring from a previously saved configuration, go to Backup and Restore.
3.1 Additional Resources

3.1.1 Netgate Training

Netgate training offers training courses for increasing your knowledge of pfSense® Plus products and services. Whether you need to maintain or improve the security skills of your staff or offer highly specialized support and improve your customer satisfaction; Netgate training has got you covered.

https://www.netgate.com/training

3.1.2 Resource Library

To learn more about how to use your Netgate appliance and for other helpful resources, make sure to browse our Resource Library.

https://www.netgate.com/resources

3.1.3 Professional Services

Support does not cover more complex tasks such as CARP configuration for redundancy on multiple firewalls or circuits, network design, and conversion from other firewalls to pfSense® Plus software. These items are offered as professional services and can be purchased and scheduled accordingly.

https://www.netgate.com/our-services/professional-services.html

3.1.4 Community Options

If you elected not to get a paid support plan, you can find help from the active and knowledgeable pfSense community on our forums.

https://forum.netgate.com/
3.2 Warranty and Support

- One year manufacturer’s warranty.
- Please contact Netgate for warranty information or view our Product Lifecycle page.
- All Specifications subject to change without notice

For support information, view our support plans.

See also:

For more information on how to use pfSense® Plus software, see the pfSense Documentation and Resource Library.