Netgate 4200 Security Gateway User Manual

Contents

1 Netgate 4200 Security Gateway
2 Product Information
3 Product Usage Instructions
4 OUT OF THE BOX
4.1 Getting Started
5 Input and Output Ports
6 Safety and Legal
7 Limited Warranty
8 HOW-TO GUIDES
9 Terminal Settings
9.1 Terminal Optimization
9.2 Launch a Terminal Program
9.3 Client-Specific Examples
9.4 GNU screen
10 Reinstalling pfSense Plus Software
10.1 Firewall Rules
10.2 Setup Policy Routing
11 Configuring an OPT interface as an additional LAN
12 Factory Reset Procedure
13 Additional Resources
14 Documents / Resources
14.1 References
15 Related Posts

Netgate 4200 Security Gateway

Product Information

- **Product Name:** Security Gateway Manual
- **Date:** Jan 08, 2024
- **Model:** Netgate-4200

Product Usage Instructions

Chapter 1: Out of the Box

Getting Started

To get started with the Security Gateway, follow these steps:

1. Download the PDF version of the Product Manual and the PDF version of the pfSense Documentation as a backup.
2. Proceed to Initial Configuration or Connecting to the USB Console Port.

What next?

To configure the firewall using a browser:

- Connect to the GUI by entering 192.168.1.1 in the address bar of a web browser.
- If a warning message appears, click the Advanced Button and then click Proceed to 192.168.1.1 (unsafe) to continue.
- If the LAN subnet IP address conflicts with the ISP-supplied modem, change the LAN interface IP address to a different subnet using the Console Menu or Setup Wizard.

Initial Configuration

Before proceeding with the initial configuration, ensure that the WAN (e.g., Fiber or Cable Modem) has a default IP Address other than 192.168.1.1 to avoid conflicting subnets on the WAN and LAN.

Connecting to the Web Interface (GUI)

1. From a computer, open a web browser and enter 192.168.1.1 in the address bar.

2. If a warning message appears, click the Advanced Button and then click Proceed to 192.168.1.1 (unsafe) to continue.

The Setup Wizard

The Setup Wizard guides you through the initial configuration of the firewall. Follow these steps:

1. Click Next to start the Setup Wizard.
2. Complete each page of the wizard to configure the firewall.
3. You can stop the wizard at any time by navigating away from the wizard pages or choosing an entry from one of the menus.

Specifications

- **Product Name:** Security Gateway Manual
- **Date:** Jan 08, 2024
- **Model:** Netgate-4200

Frequently Asked Questions (FAQ)

Q: Can I use the default IP address on both WAN and LAN?
A: No, the default IP address on the ISP-supplied modem and the Netgate firewall LAN interface cannot be the same. If they are conflicting, change the LAN interface IP address to a different subnet.

Q: How do I change the interface IP address?
A: You can change the interface IP address using either the Console Menu or the Setup Wizard. From the Console Menu, choose option 2 and follow the steps to change it. From the GUI, go to System > Setup Wizard and change the IP address on Step 5. Save the changes after completing the Wizard.

Q: What should I do if I encounter a certificate warning message?
A: If a certificate warning message appears, click the Advanced Button and then click Proceed to 192.168.1.1 (unsafe) to continue.

Security Gateway Manual

This Quick Start Guide covers the first time connection procedures for the Netgate® 4200 Desktop Firewall Appliance and will provide the information needed to keep the appliance up and running.

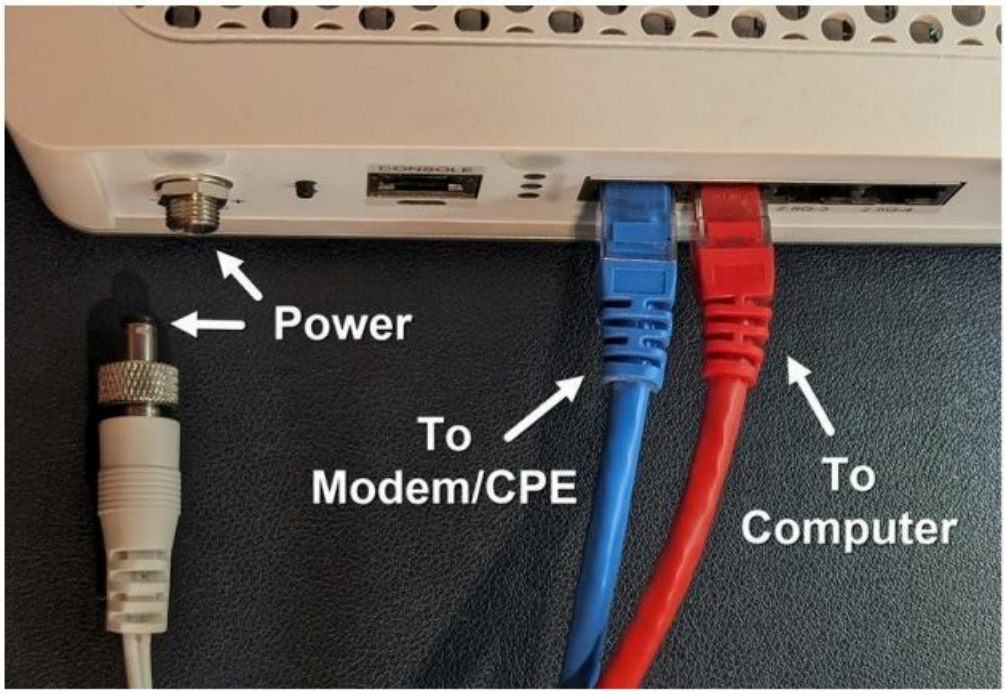
Tip: Before getting started, a good practice is to download the PDF version of the Product Manual and the PDF version of the pfSense Documentation in case Internet access is not available during setup.

OUT OF THE BOX

Getting Started

The basic firewall configuration begins with connecting the Netgate® appliance to the Internet. The Netgate appliance should be unplugged at this time.
Connect one end of an Ethernet cable to the WAN port (shown in the Input and Output Ports section) of the Netgate appliance. The other end of the same cable should be inserted into a LAN port on the ISP CPE device,

such as a cable or fiber modem. If the CPE device provided by the ISP has multiple LAN ports, any LAN port should work in most circumstances.
Next, connect one end of a 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 computer.



What next?

To connect to the GUI and configure the firewall in a browser, continue on to Initial Configuration.
To connect to the console and make adjustments before connecting to the GUI, see Connecting to the USB Console Port.
Warning: The default IP Address on the LAN subnet on the Netgate firewall is 192.168.1.1/24. The same subnet cannot be used on both WAN and LAN, so if the default IP address on the ISP-supplied modem is also 192.168.1.1/24, disconnect theWAN interface until the LAN interface on the firewall has been renumbered to a different subnet (like 192.168.2.1/24) to avoid an IP Address conflict.
To change an interface IP address, choose option 2 from the Console Menu and walk through the steps to change it, or from the GUI, go through the Setup Wizard (opens at first boot, also found at System > Setup Wizard) and change the IP address on Step 5. Complete the Wizard and save the changes.

Initial Configuration
Plug the power cable into the power port (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 the CPE on WAN (e.g. Fiber or Cable Modem) has a default IP Address of 192.168.1.1, disconnect the Ethernet cable from the 1 port on the Netgate 4200 Security Gateway before proceeding.
Change the default LAN IP Address of the device during a later step in the configuration to avoid having conflicting subnets on the WAN and LAN.

Connecting to the Web Interface (GUI)

1. From the computer, log into the web interface

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

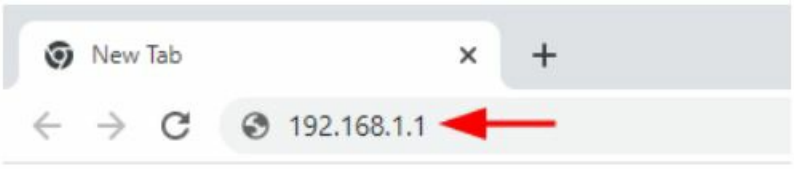


Fig. 1: Enter the default LAN IP address in the browser

2. A warning message may appear. If this message or similar message is encountered, it is safe to proceed. Click the Advanced Button and then 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

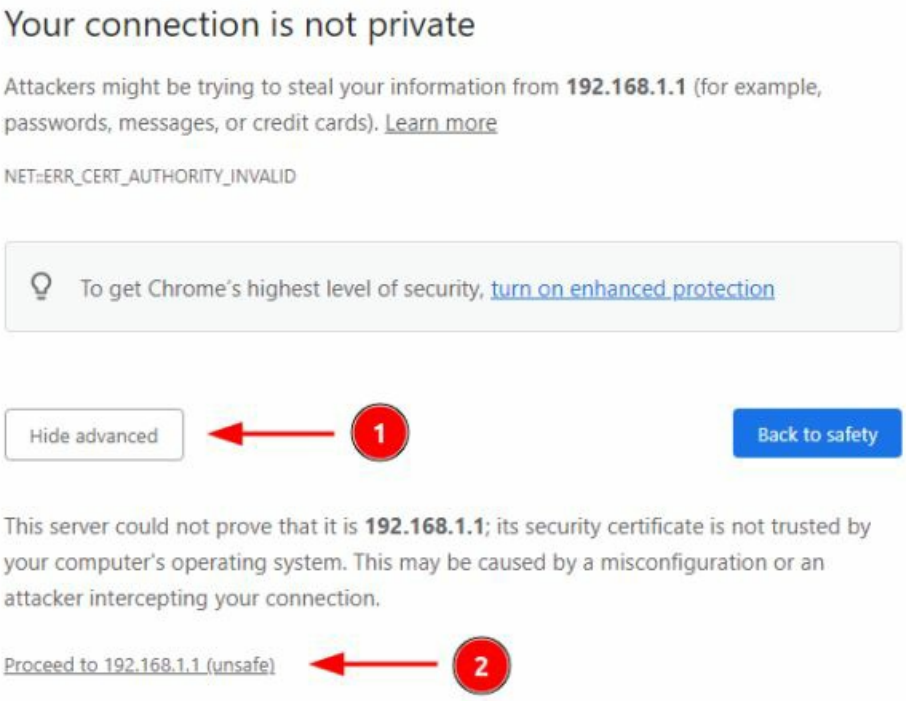


Fig. 2: Example certificate warning message

The Setup Wizard
This section steps through each page of the Setup Wizard to perform the initial configuration of the firewall. The wizard collects information one page at a time but it does not make any changes to the firewall until the wizard is completed.

Tip: The wizard can be safely stopped at any time for those who wish to perform the configuration manually or restore an existing backup (Backup and Restore).
To stop the wizard, navigate away from the wizard pages by clicking the logo in the upper left of the page or by choosing an entry from one of the menus.

Note: Ignore the warning at the top of each wizard page about resetting the admin account password. One of the steps in the Setup Wizard is to change the default password, but the new password is not applied until the end of the wizard.

1. Click Next to start the Setup Wizard.

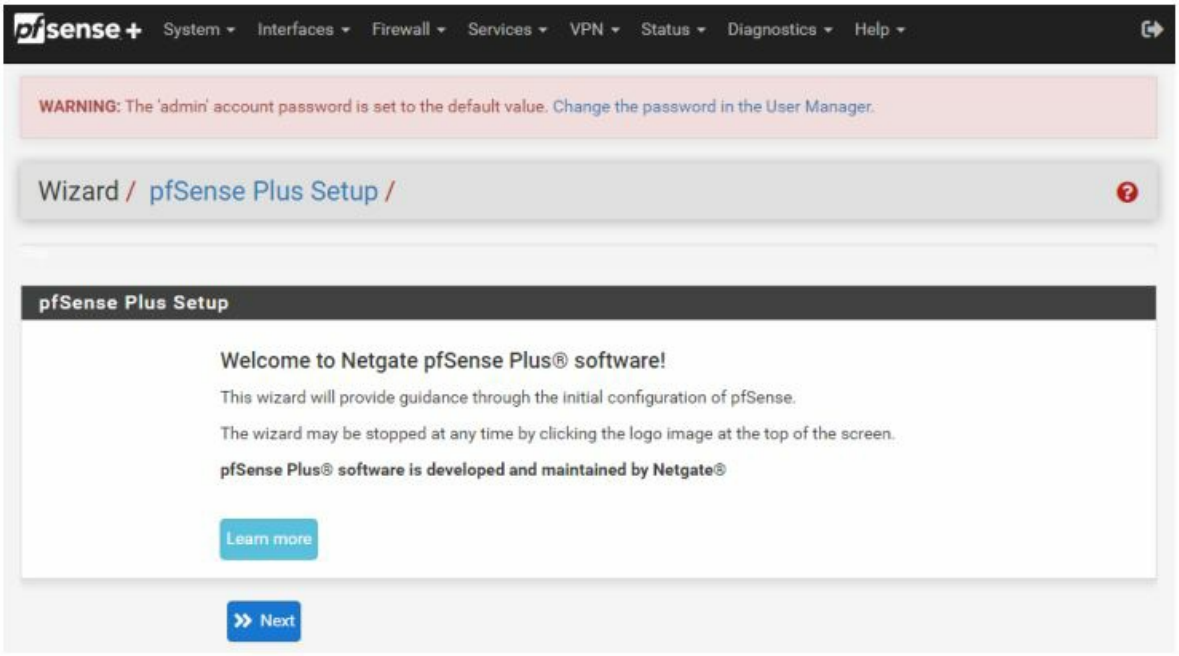


Fig. 3: Setup Wizard starting page

2. Click Next after reading the information on Netgate Global Support.
3. Use the following items as a guide to configure the options on the General Information page:
   Hostname Any desired hostname name can be entered to identify the firewall. For the purposes of this guide, the default hostname pfsense is used.
   Domain The domain name under which the firewall operates. The default home.arpa 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).
   Note: The firewall defaults to acting as a resolver and clients will not utilize these forwarding DNS servers. However, these servers give the firewall itself a way to ensure it has working DNS if resolving the default way does not work properly.

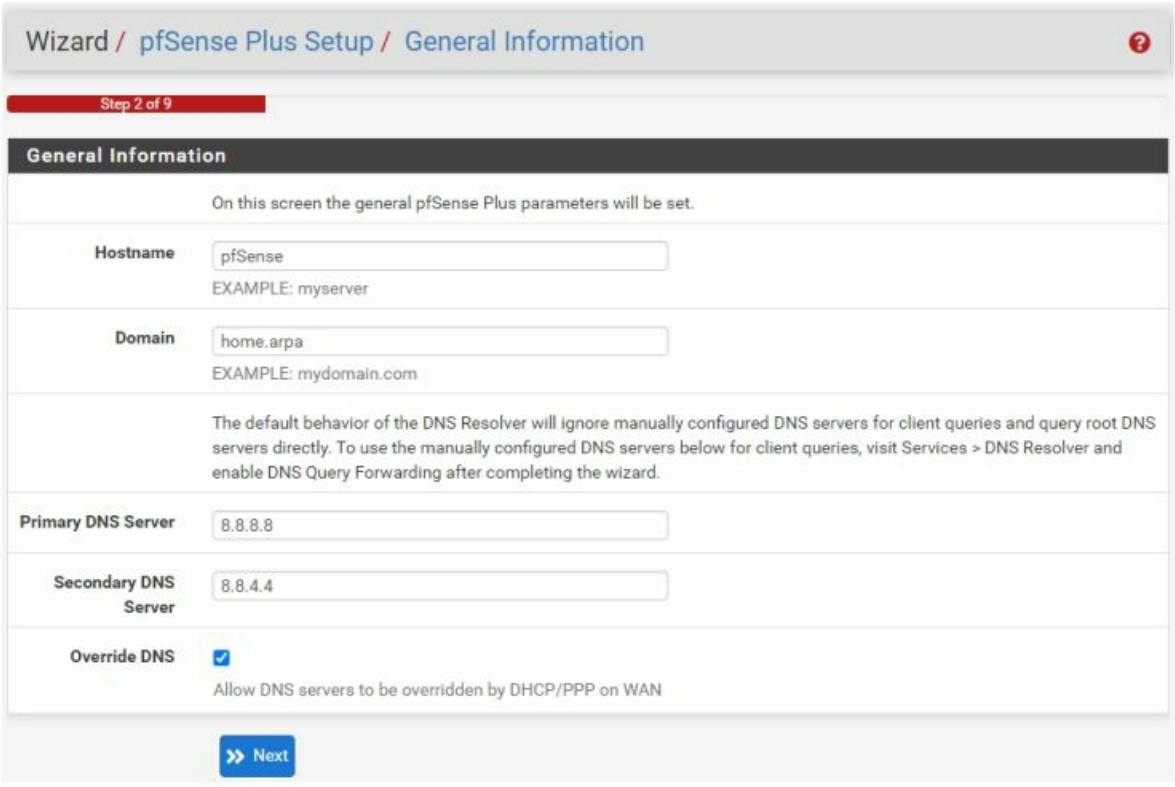


Fig. 4: **General Information** page in the Setup Wizard

Type in the DNS Server information and Click Next.

4. Use the following information for the Time Server Information page:

   Time Server Hostname Use the default time server address. The default hostname is suitable for both IPv4 and IPv6 NTP clients.

   Timezone Select a geographically named time zone for the location of the firewall.

   For this guide, the Timezone will be set to America/Chicago for US Central time.

   Change the Timezone and click Next.

5. Use the following information for the Configure WAN Interface page:

   The WAN interface is the external (public) IP address the firewall will use to communicate with the Internet.

   DHCP is the default and is the most common type of WAN interface for home fiber and cable modems.

   Default settings for the other items on this page should be acceptable for normal home users.

   Default settings should be acceptable. Click Next.

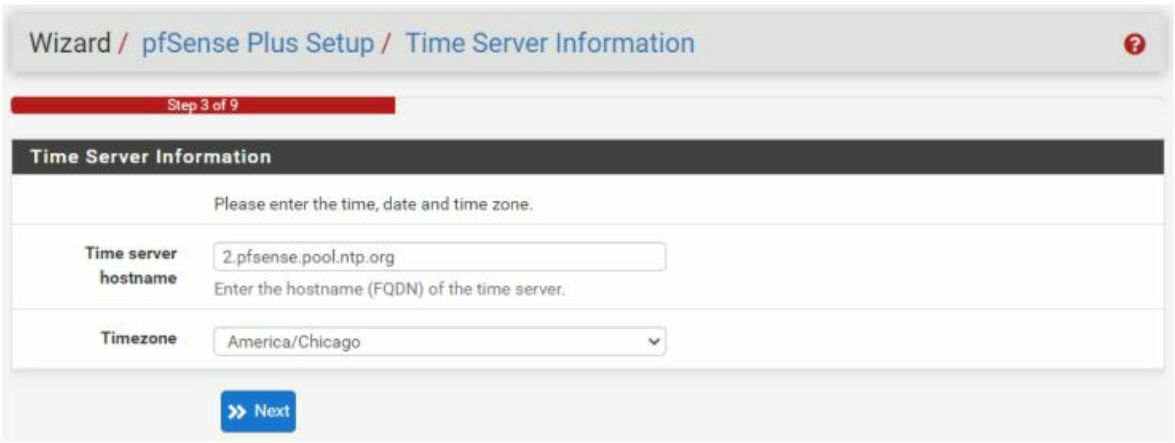


Fig. 5: **Time Server Information** page in the Setup Wizard

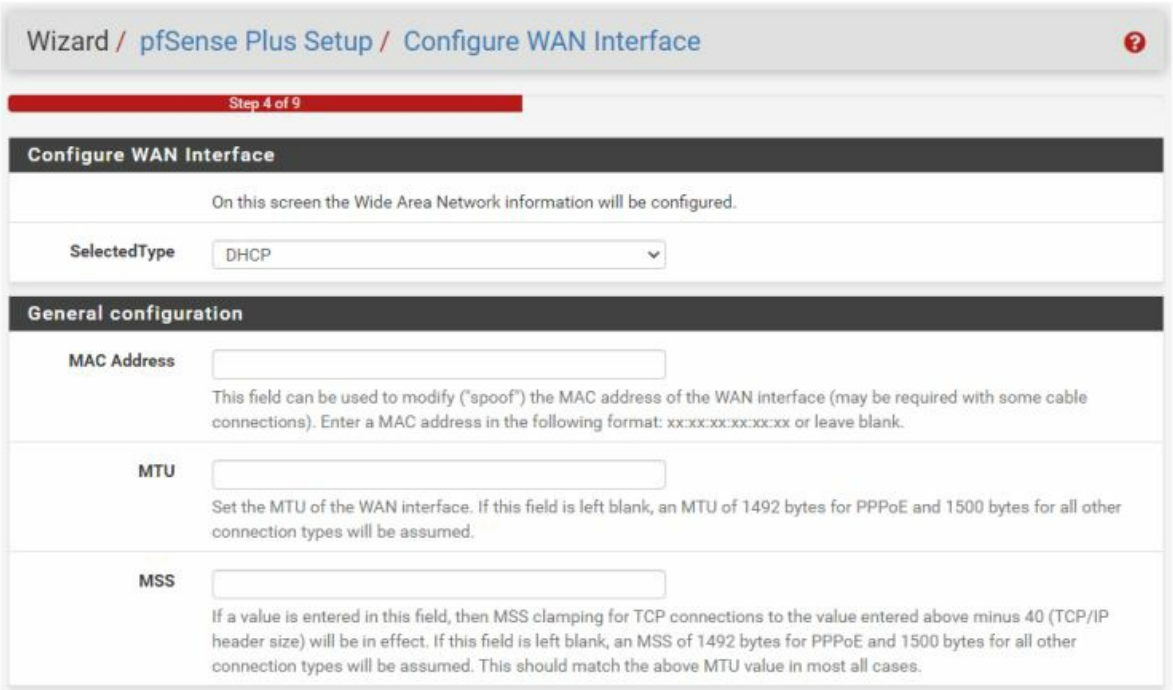


Fig. 6: **Configure WAN Interface** page in the Setup Wizard

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 the CPE on WAN (e.g. Fiber or Cable Modem) has a default IP Address of 192.168.1.1, the Ethernet cable should be disconnected from the 1 port on the Netgate 4200 Security Gateway before starting.

Change the default LAN IP Address of the device during this step in the configuration to avoid having conflicting subnets on the WAN and LAN.

7. Change the Admin Password. Enter the same new 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.

Note: This step of the wizard also contains several useful links to Netgate resources and methods of obtaining assistance with the product. Be sure to read through the items on this page before finishing the wizard.

Finishing Up
After completing or exiting the wizard, during the first time loading the Dashboard the firewall will display a notification modal dialog with the Copyright and Trademark Notices.
Read and click Accept to continue to the dashboard.
If the Ethernet cable was unplugged at the beginning of this configuration, reconnect it to the 1 port now.
This completes the basic configuration for the Netgate appliance.

pfSense Plus Software 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.

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.

- Section 1 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.

Fig. 7: Copyright and Trademark Notices

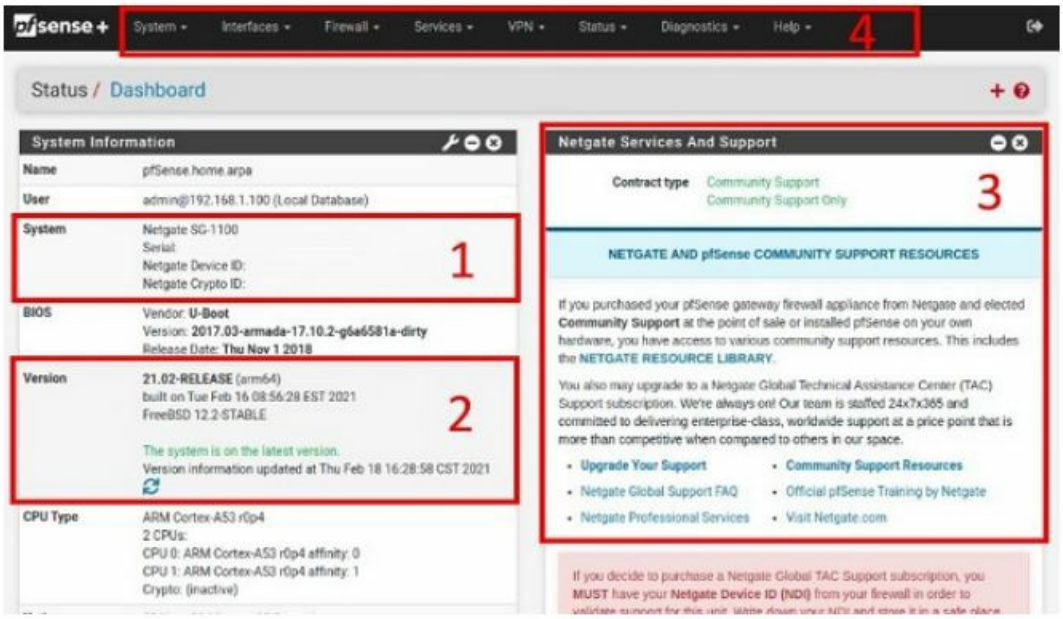


Fig. 8: The pfSense® Plus Dashboard

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

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.

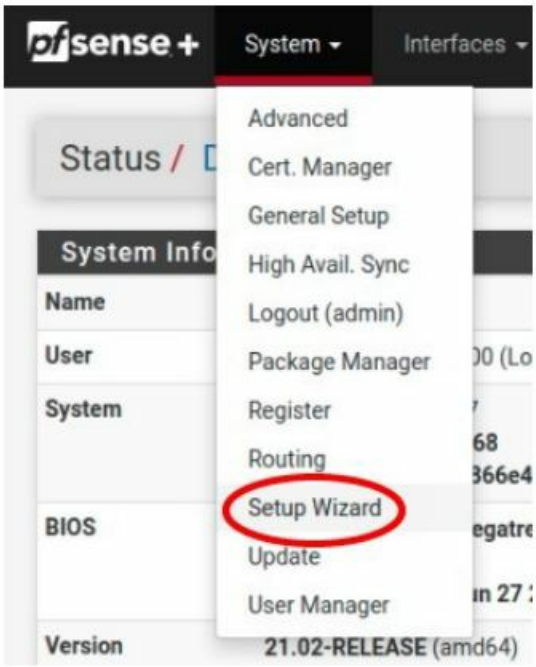


Fig. 9: Re-run the Setup Wizard

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 USB Console Port. Cable is required.
Tip: To learn more about getting the most out of a Netgate appliance, sign up for a pfSense Plus Software Training course or browse the extensive Resource Library.

Updates
When a new version of pfSense Plus software is available, the device will indicate the availability of the new version on the System Information dashboard widget. Users can peform a manual check as well by visiting System > Update.
Users can initiate an upgrade from the System > Update page as needed.
For more information, see the Upgrade Guide.

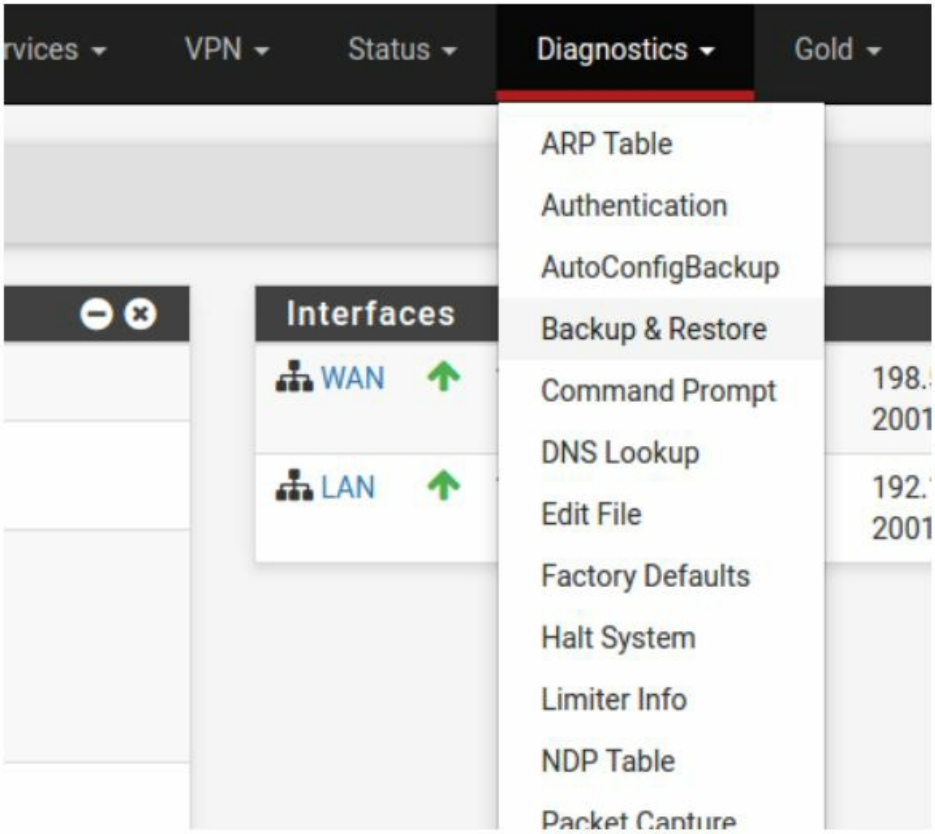


Fig. 10: Backup & Restore

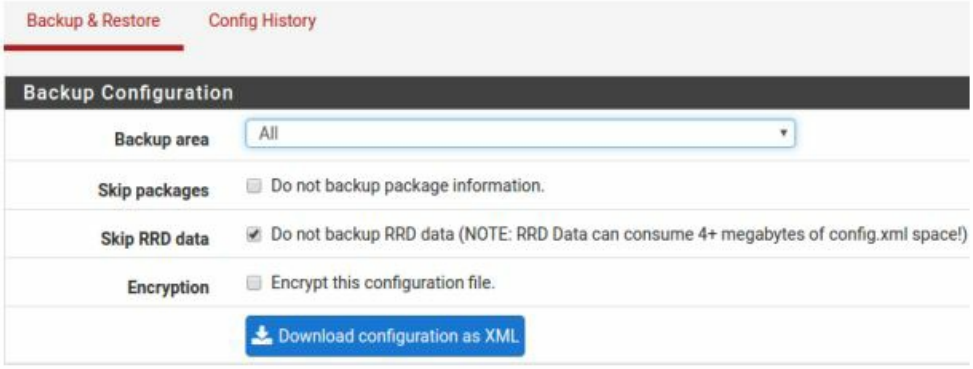


Fig. 11: Click Download configuration as XML

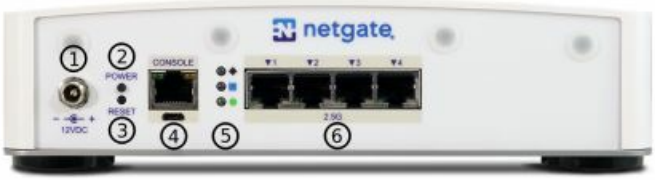


Fig. 12: Rear view of the Netgate 4200 Firewall Appliance

Input and Output Ports

Rear Side
The rear side of the Netgate 4200 contains several items of interest for connecting to and managing the device.

Fig. 13: Front view of the Netgate 4200 Firewall Appliance

The items below are marked with circled numbers on figure Rear view of the Netgate 4200 Firewall Appliance:

Item	Description
1	Power Connector
2	ACPI Power Button (Protruding) – Graceful shutdown, hard power off (Hold 10s), power on
3	Reset Button (Recessed) – Used when performing the ***Factory Reset Procedure***.
4	Serial Console (***USB*** or ***RJ45***)
5	Rear ***Status LEDs***
6	***Networking Ports***

- Power Connector (1) The Power connector is 12VDC with threaded locking connector. Power consumption is approximately 13W when idle.
- Power Button (2) The upper protruding Power Button behaves the same as a typical ACPI power button.
  If the device is powered on and running, pressing the button immediately performs a graceful shutdown and the system enters a standby state.
  If the system is in a powered off or standby state, pressing the power button immediately powers on the device and starts the boot process.
  If the system is unresponsive, holding in the power button for 10 seconds will forcefully power off the device. Press the power button again to turn it back on.
- Reset Button (3) The lower recessed Reset Button is used to perform the Factory Reset Procedure.
  Pressing and immediately releasing the button has no effect, it does not perform a hardware reset.
  See Factory Reset Procedure for details on how to use the button to perform a factory reset.
- Serial Console Port (4) Clients can access the serial console using the USB Micro-B (5-pin) serial adapter port and a compatible USB cable or via the RJ45 “Cisco” style port with a separate cable and USB serial adapter or client hardware port.

Note: Only one type of console connection will work at a time and the RJ45 console connection has priority. If both ports are connected only the RJ45 console port will function.

Note: The serial console in the OS is a memory mapped serial port and not a traditional COM port. pfSense® Plus automatically detects and uses the correct console type for this device.

Note: The RJ45 Serial Console port is only for use with the Serial Console. It cannot be used for any other

purpose.
Status LEDs (5) The rear status LEDs show the same output as the status LEDs on the front of the unit. See Status LEDs for information on interpreting the meaning of different LED states.
Networking Ports (6) This group of four ports are the network interfaces. They are explained in detail in the next section, Networking Ports.

Networking Ports
The section on the rear of the device numbered 6 in Rear view of the Netgate 4200 Firewall Appliance contains the network interfaces. These ports are labeled 1 through 4 on the device.

Label	Assigned Name	Device Name	Type	Speed
1	PORT1WAN	igc3	RJ-45	2.5 Gbps
2	PORT2LAN	igc2	RJ-45	2.5 Gbps
3	PORT3	igc1	RJ-45	2.5 Gbps
4	PORT4	igc0	RJ-45	2.5 Gbps

Note: The igc(4) network interfaces on this device do not support fixed speed operation. These interfaces emulate a speed/duplex choice by limiting the values offered during autonegotiation to the speed/duplex value selected in the GUI.
When connecting different devices to these interfaces the peer should typically be set to autonegotiate, not to a specific speed or duplex value. The exception to this is if the peer interface has the same limitation, in which case both peers should select the same negotiation speed.

Front Side
The front of the device has Status LEDs as well as an access panel for future expansion uses.

Fig. 13: Front view of the Netgate 4200 Firewall Appliance

Right Side

Fig. 14: Right side view of the Netgate 4200 Firewall Appliance

The right side panel of the device (when facing the front) contains:

#	Description	Purpose
1	USB 3.0 Port	Connect USB devices

USB Ports
USB ports on the device can be used for a variety of purposes.
The primary use for the USB ports is to install or reinstall the operating system on the device. Beyond that, there are numerous USB devices which can expand the base functionality of the hardware, including some supported by add-on packages. For example, UPS/Battery Backups, Cellular modems, GPS units, and storage devices. Though the operating system also supports wired and wireless network devices, these are not ideal and should be avoided.

Status LEDs
The Netgate 4200 has two sets of status LEDs: One on the front of the device and one on the rear. The status LEDs on the front are horizontal while the LEDs on the rear are arranged vertically. Though the placement is different, both sets are labeled consistently.

LED Patterns

Description	LED Pattern
Standby	Circle pulsing orange
Boot in Process	Diamond flashing blue
Boot Completed/Ready	Diamond solid blue
Upgrade Available	Square solid purple
Upgrade in Progress	All rapidly flash green
Triggering Reset	Circle, Square, then Diamond solid red (***Factory Reset Procedure***)
Reset In Progress	All rapidly flash red (***Factory Reset Procedure***)

Fig. 15: Status LEDs on the front (left) and rear (right) of the Netgate 4200 Firewall Appliance

Safety and Legal

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.

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.
    - 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.
    - 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.
    - Contact a qualified electrician or the manufacturer if there are questions about the installation prior to connecting the equipment.
    - Protective grounding/earthing is provided by Listed AC adapter. Building installation shall provide appropriate short-circuit backup protection.
    - Protective bonding must be installed in accordance with local national wiring rules and regulations.
      Warning: To help protect your Netgate appliance from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, uninterruptible power supply (UPS) or a combination of those devices.
      Failure to take such precautions could result in premature failure, and/or damage to your Netgate appliance, which is not covered under the product warranty. Such an event may also present the risk of electric shock, fire, or explosion.

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.

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.

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

RoHS/WEEE Compliance Statement

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.

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
Austin, Texas 78728
legal@netgate.com
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.

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.

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.

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.

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 ORWARRANTIES 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, IMPLIEDWARRANTIES 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 ANY 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.

HOW-TO GUIDES

Connecting to the USB Console Port
This guide shows how to access the serial console which can be used for troubleshooting and diagnostics tasks as well as some basic configuration.

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

Install the Driver

A Silicon Labs CP210x USB-to-UART Bridge driver is used to provide access to the console, which is exposed via the USB Micro-B (5-pin) port on the appliance.
If needed, install an appropriate Silicon Labs CP210x USB to UART Bridge driver on the workstation used to connect with the device.

Windows
There are drivers available for Windows available for download.

macOS
There are drivers available for macOS available for download.
For macOS, choose the CP210x VCP Mac download.

Linux
There are drivers available for Linux available for download.

FreeBSD
Recent versions of FreeBSD include this driver and will not require manual installation.

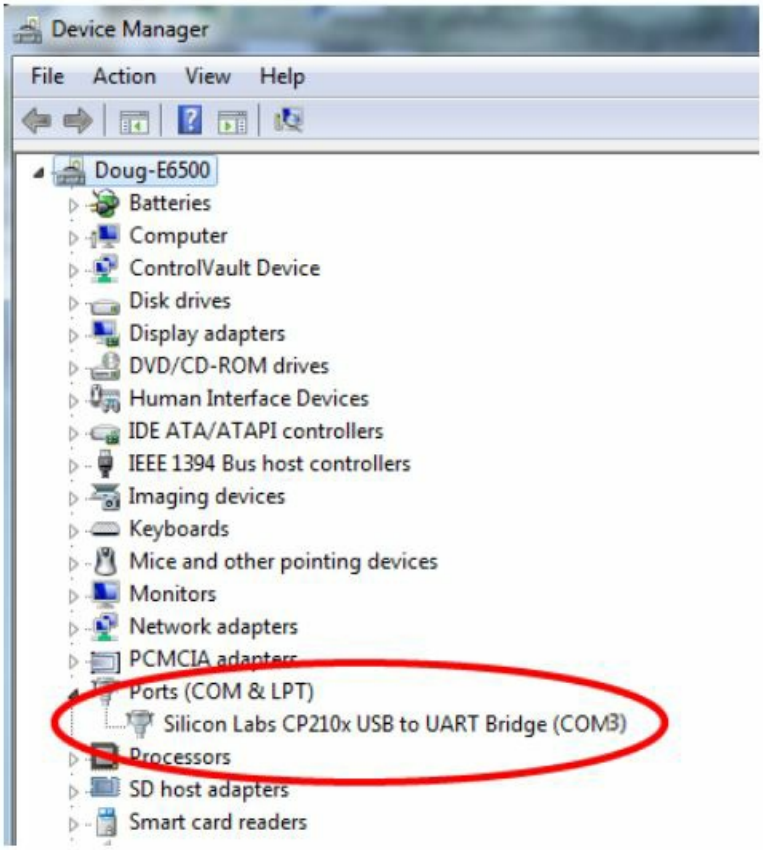
Connect a USB Cable
Next, locate an appropriate USB cable that has a USB Micro-B (5-pin) connector on one end and a regular USB Type A plug on the other end. These cables are commonly used with smaller USB peripherals such as GPS units, cameras, and so on.
Gently push the USB Micro-B (5-pin) plug end into the console port on the appliance and connect the USB Type A plug into an available USB port on the workstation.

Tip: Be certain to gently push in the USB Micro-B (5-pin) connector on the device side completely. With most cables there will be a tangible “click”, “snap”, or similar indication when the cable is fully engaged.

Apply Power to the Device
On some devices when using a USB serial console port the serial port will not appear on the client operating system until the device is plugged into a power source.
If the client OS does not see the serial device, connect the power cord to the device to allow it to start booting.
If the device appears without power, then better to wait until the terminal is open before connecting power so the client can view the entire boot output.

Locate the Console Port Device
The appropriate console port device that the workstation assigned as the serial port must be located before attempting to connect to the console.
Note: Even if the serial port was assigned in the BIOS, the workstation OS may remap it to a different COM Port.

Windows
To locate the device name on Windows, open Device Manager and expand the section for Ports (COM & LPT). Look for an entry with a title such as Silicon Labs CP210x USB to UART Bridge. If there is a label in the name that contains “COMX” where X is a decimal digit (e.g. COM3), that value is what would be used as the port in the terminal program.



macOS
The device associated with the system console is likely to show up as, or start with, /dev/cu.usbserial-<id>.
Run ls -l /dev/cu.* from a Terminal prompt to see a list of available USB serial devices and locate the appropriate one for the hardware. If there are multiple devices, the correct device is likely the one with the most recent timestamp or highest ID.

Linux
The device associated with the system console is likely to show up as /dev/ttyUSB0. Look for messages about the device attaching in the system log files or by running dmesg.
Note: If the device does not appear in /dev/, see the note above in the driver section about manually loading the Linux driver and then try again.

FreeBSD
The device associated with the system console is likely to show up as /dev/cuaU0. Look for messages about the device attaching in the system log files or by running dmesg.
Note: If the serial device is not present, ensure the device has power and then check again.

Launch a Terminal Program
Use a terminal program to connect to the system console port. Some choices of terminal programs:

Windows
For Windows the best practice is to run PuTTY in Windows or SecureCRT. An example of how to configure PuTTY is below.

Warning: Do not use Hyperterminal.

macOS
For macOS the best practice is to run GNU screen, or cu. An example of how to configure GNU screen is below.
Linux
For Linux the best practices are to run GNU screen, PuTTY in Linux, minicom, or dterm. Examples of how to configure PuTTY and GNU screen are below.

FreeBSD
For FreeBSD the best practice is to run GNU screen or cu. An example of how to configure GNU screen is below.

Client-Specific Examples

PuTTY in Windows

- Open PuTTY and select Session under Category on the left hand side.
- Set the Connection type to Serial
- Set Serial line to the console port determined previously
- Set the Speed to 115200 bits per second.
- Click the Open button

PuTTY will then display the console.

PuTTY in Linux

- Open PuTTY from a terminal by typing sudo putty

  Note: The sudo command will prompt for the local workstation password of the current account.
- Set the Connection type to Serial
- Set Serial line to /dev/ttyUSB0
- Set the Speed to 115200 bits per second
- Click the Open button

PuTTY will then display the console.

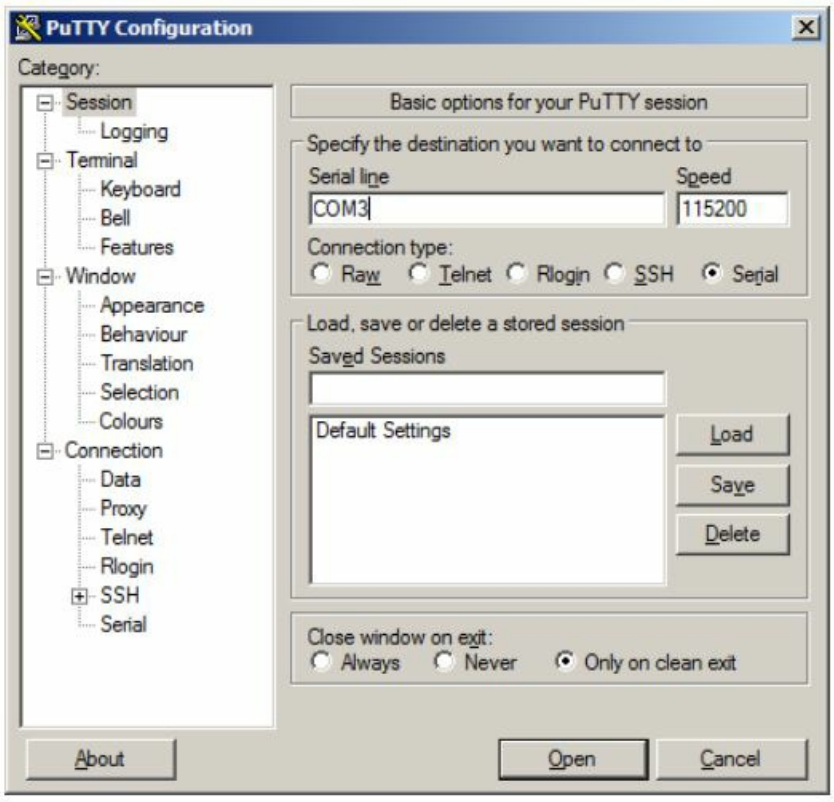


Fig. 1: An example of using PuTTY in Windows

Fig. 2: An example of using PuTTY in Linux

GNU screen
In many cases screen may be invoked simply by using the proper command line, where <console-port> is the console port that was located above.

```
$ sudo screen <console-port> 115200
```

Note: The sudo command will prompt for the local workstation password of the current account.

If portions of the text are unreadable but appear to be properly formatted, the most likely culprit is a character encoding mismatch in the terminal. Adding the -U parameter to the screen command line arguments forces it to use UTF-8 for character encoding:

```
$ sudo screen -U <console-port> 115200
```

Terminal Settings

The settings to use within the terminal program are:

- Speed 115200 baud, the speed of the BIOS
- Data bits 8
- Parity None
- Stop bits 1
- Flow Control Off or XON/OFF.

Warning: Hardware flow control (RTS/CTS) must be disabled.

Terminal Optimization

Beyond the required settings there are additional options in terminal programs which will help input behavior and output rendering to ensure the best experience. These settings vary location and support by client, and may not be available in all clients or terminals.

These are:

- Terminal Type xterm
  This setting may be under Terminal, Terminal Emulation, or similar areas.
- Color Support ANSI colors / 256 Color / ANSI with 256 Colors
  This setting may be under Terminal Emulation, Window Colors, Text, Advanced Terminfo, or similar areas.
- Character Set / Character Encoding UTF-8
  This setting may be under Terminal Appearance, Window Translation, Advanced International, or similar areas.
  In GNU screen this is activated by passing the -U parameter.
- Line Drawing Look for and enable setting such as “Draw lines graphically”, “Use unicode graphics characters”, and/or “Use Unicode line drawing code points”.
  These settings may be under Terminal Appearance, Window Translation, or similar areas.
- Function Keys / Keypad Xterm R6
  In Putty this is under Terminal > Keyboard and is labeled The Function Keys and Keypad.
- Font For the best experience, use a modern monospace unicode font such as Deja Vu Sans Mono, Liberation Mono, Monaco, Consolas, Fira Code, or similar.
  This setting may be under Terminal Appearance, Window Appearance, Text, or similar areas.

What’s Next?
After connecting a terminal client, it may not immediately see any output. This could be because the device has already finished booting or it may be that the device is waiting for some other input.
If the device does not yet have power applied, plug it in and monitor the terminal output.
If the device is already powered on, try pressing Space. If there is still no output, press Enter. If the device was booted, it may redisplay the console menu or login prompt, or produce other output indicating its status.
From the console, a variety of things are possible, such as changing interface addresses. There is a full explanation of every console menu option in the pfSense software documentation.

Troubleshooting

Serial Device Missing
With a USB serial console there are a few reasons why the serial port may not be present in the client operating system, including:

- **No Power** Some models require power before the client can connect to the USB serial console.
- **USB Cable Not Plugged In** For USB consoles, the USB cable may not be fully engaged on both ends. Gently, but firmly, ensure the cable has a good connection on both sides.
  Bad USB Cable Some USB cables are not suitable for use as data cables. For example, some cables are only capable of delivering power for charging devices and not acting as data cables. Others may be of low quality or have poor or worn connectors.
  The ideal cable to use is the one that came with the device. Failing that, ensure the cable is of the correct type and specifications, and try multiple cables.
- **Wrong Device** In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.
- **Hardware Failure** There could be a hardware failure preventing the serial console from working. Contact Netgate TAC for assistance.

No Serial Output

If there is no output at all, check the following items:

- **USB Cable Not Plugged In** For USB consoles, the USB cable may not be fully engaged on both ends. Gently, but firmly, ensure the cable has a good connection on both sides.
  Wrong Device In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.
- **Wrong Terminal Settings** Ensure the terminal program is configured for the correct speed. The default BIOS speed is 115200, and many other modern operating systems use that speed as well.
  Some older operating systems or custom configurations may use slower speeds such as 9600 or 38400.
- **Device OS Serial Console Settings** Ensure the operating system is configured for the proper console (e.g. ttyS1 in Linux). Consult the various operating install guides on this site for further information.

PuTTY has issues with line drawing

PuTTY generally handles most cases OK but can have issues with line drawing characters on certain platforms. These settings seem to work best (tested on Windows):

- Window
  - Columns x Rows 80×24
- Window > Appearance
  - Font Courier New 10pt or Consolas 10pt
- Window > Translation
  - Remote Character Set Use font encoding or UTF-8
  - Handling of line drawing characters Use font in both ANSI and OEM modes or Use Unicode line drawing code points
- Window > Colours
  Indicate bolded text by changing The colour

Garbled Serial Output
If the serial output appears to be garbled, missing characters, binary, or random characters check the following items:

Flow Control In some cases flow control can interfere with serial communication, causing dropped characters or other issues. Disabling flow control in the client can potentially correct this problem.
On PuTTY and other GUI clients there is typically a per-session option to disable flow control. In PuTTY, the Flow Control option is in the settings tree under Connection, then Serial.
To disable flow control in GNU Screen, add the -ixon and/or -ixoff parameters after the serial speed as in the following example:

```
$ sudo screen <console port> 115200,-ixon
```

- **Terminal Speed** Ensure the terminal program is configured for the correct speed. (See No Serial Output)
- **Character Encoding** Ensure the terminal program is configured for the proper character encoding, such as

UTF-8 or Latin-1, depending on the operating system. (See GNU Screen)

Serial Output Stops After the BIOS
If serial output is shown for the BIOS but stops afterward, check the following items:

- **Terminal Speed** Ensure the terminal program is configured for the correct speed for the installed operating system.
  (See No Serial Output)
- **Device OS Serial** Console Settings Ensure the installed operating system is configured to activate the serial console and that it is configured for the proper console (e.g. ttyS1 in Linux). Consult the various operating install guides on this site for further information.
- **Bootable Media** If booting from a USB flash drive, ensure that the drive was written correctly and contains a bootable operating system image.

Connecting to the RJ45 Console Port

There are times when directly accessing the console is required. Perhaps GUI or SSH access has been locked out, or
the password has been lost or forgotten.
A separate adapter is required to make a connection between a computer and the firewall using the RJ45 serial port.
This can be a direct RJ45-to-USB serial adapter or a standard USB-to-serial adapter and an RJ45-to-DB9 adapter or cable. It is also possible to utilize client hardware serial ports and compatible cables, but these ports are rare on modern hardware.
These are standard components, inexpensive and readily available from most retail outlets that sell computer cables.
Installing drivers and locating the port will vary depending on the third party device, consult its documentation for details.

Launch a Terminal Program

Use a terminal program to connect to the system console port. Some choices of terminal programs:

Windows
For Windows the best practice is to run PuTTY in Windows or SecureCRT. An example of how to configure PuTTY is below.

Warning: Do not use Hyperterminal.

macOS
For macOS the best practice is to run GNU screen, or cu. An example of how to configure GNU screen is below.

Linux
For Linux the best practices are to run GNU screen, PuTTY in Linux, minicom, or dterm. Examples of how to configure PuTTY and GNU screen are below.

FreeBSD
For FreeBSD the best practice is to run GNU screen or cu. An example of how to configure GNU screen is below.

Client-Specific Examples

PuTTY in Windows

- Open PuTTY and select Session under Category on the left hand side.
- Set the Connection type to Serial
- Set Serial line to the console port determined previously
- Set the Speed to 115200 bits per second.
- Click the Open button

PuTTY will then display the console.

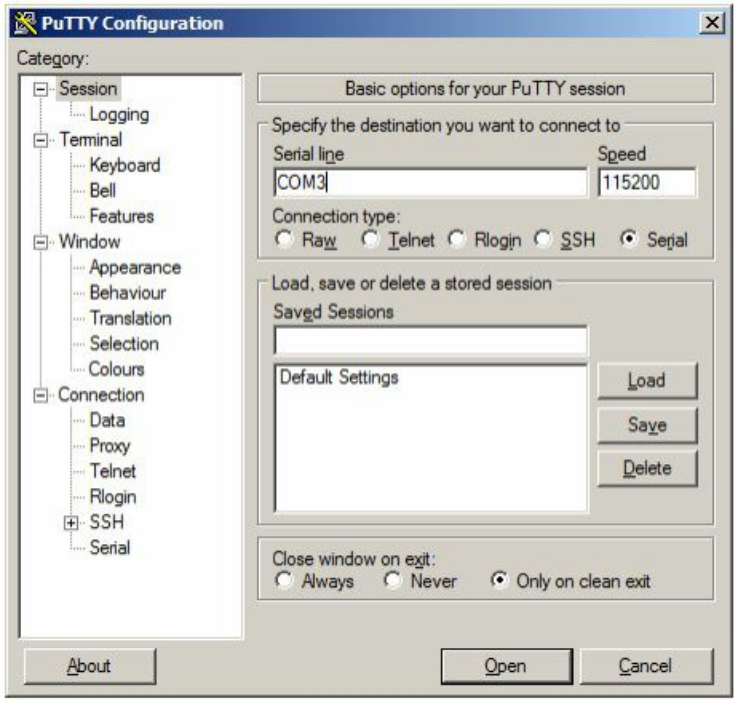


Fig. 3: An example of using PuTTY in Windows

PuTTY in Linux

- Open PuTTY from a terminal by typing sudo putty

Note: The sudo command will prompt for the local workstation password of the current account.

- Set the Connection type to Serial
- Set Serial line to /dev/ttyUSB0
- Set the Speed to 115200 bits per second
- Click the Open button

PuTTY will then display the console.

Fig. 4: An example of using PuTTY in Linux

GNU screen

In many cases screen may be invoked simply by using the proper command line, where <console-port> is the console port that was located above.

```
$ sudo screen <console-port> 115200
```

If portions of the text are unreadable but appear to be properly formatted, the most likely culprit is a character encoding mismatch in the terminal. Adding the -U parameter to the screen command line arguments forces it to use UTF-8 for character encoding:

```
$ sudo screen -U <console-port> 115200
```

To disable flow control in GNU Screen, add the -ixon and/or -ixoff parameters after

Terminal Settings

The settings to use within the terminal program are:

- Speed 115200 baud, the speed of the BIOS
- Data bits 8
- Parity None
- Stop bits 1
- Flow Control Off or XON/OFF.

Warning: Hardware flow control (RTS/CTS) must be disabled.

Terminal Optimization
Beyond the required settings there are additional options in terminal programs which will help input behavior and output rendering to ensure the best experience. These settings vary location and support by client, and may not be
available in all clients or terminals.

These are:

- Terminal Type xterm
  This setting may be under Terminal, Terminal Emulation, or similar areas.
- **Color Support** ANSI colors / 256 Color / ANSI with 256 Colors
  This setting may be under Terminal Emulation, Window Colors, Text, Advanced Terminfo, or similar areas.
- **Character Set** / **Character Encoding** UTF-8
  This setting may be under Terminal Appearance, Window Translation, Advanced International, or similar areas.
  In GNU screen this is activated by passing the -U parameter.
- **Line Drawing** Look for and enable setting such as “Draw lines graphically”, “Use unicode graphics characters”, and/or “Use Unicode line drawing code points”.
  These settings may be under Terminal Appearance, Window Translation, or similar areas.
- **Function Keys** / **Keypad** Xterm R6
  In Putty this is under Terminal > Keyboard and is labeled The Function Keys and Keypad.
- **Font** For the best experience, use a modern monospace unicode font such as Deja Vu Sans Mono, Liberation Mono, Monaco, Consolas, Fira Code, or similar.
  This setting may be under Terminal Appearance, Window Appearance, Text, or similar areas.

What’s Next?

After connecting a terminal client, it may not immediately see any output. This could be because the device has already finished booting or it may be that the device is waiting for some other input.
If the device does not yet have power applied, plug it in and monitor the terminal output.
If the device is already powered on, try pressing Space. If there is still no output, press Enter. If the device was booted, it may redisplay the console menu or login prompt, or produce other output indicating its status.
From the console, a variety of things are possible, such as changing interface addresses. There is a full explanation of every console menu option in the pfSense software documentation.

Troubleshooting

Serial Device Missing

With a USB serial console there are a few reasons why the serial port may not be present in the client operating system, including:

- **No Power** Some models require power before the client can connect to the USB serial console.
- **USB Cable Not Plugged** In For USB consoles, the USB cable may not be fully engaged on both ends. Gently, but firmly, ensure the cable has a good connection on both sides.
- **Bad USB Cable Some** USB cables are not suitable for use as data cables. For example, some cables are only capable of delivering power for charging devices and not acting as data cables. Others may be of low quality or have poor or worn connectors.
  The ideal cable to use is the one that came with the device. Failing that, ensure the cable is of the correct type and specifications, and try multiple cables.
  Wrong Device In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.
- **Hardware Failure** There could be a hardware failure preventing the serial console from working. Contact Netgate TAC for assistance.

No Serial Output

If there is no output at all, check the following items:

- **USB Cable Not Plugged In** For USB consoles, the USB cable may not be fully engaged on both ends. Gently, but firmly, ensure the cable has a good connection on both sides.
- **Wrong Device** In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.
- **Wrong Terminal Settings** Ensure the terminal program is configured for the correct speed. The default BIOS speed is 115200, and many other modern operating systems use that speed as well.
  Some older operating systems or custom configurations may use slower speeds such as 9600 or 38400.
- **Device OS Serial Console** Settings Ensure the operating system is configured for the proper console (e.g. ttyS1 in Linux). Consult the various operating install guides on this site for further information.

PuTTY has issues with line drawing
PuTTY generally handles most cases OK but can have issues with line drawing characters on certain platforms. These settings seem to work best (tested on Windows):

- **Window**
  - Columns x Rows 80×24
- Window > Appearance
  - Font Courier New 10pt or Consolas 10pt
- Window > Translation
  - Remote Character Set Use font encoding or UTF-8
  - Handling of line drawing characters Use font in both ANSI and OEM modes or Use Unicode line drawing code points
- Window > Colours
  - Indicate bolded text by changing The colour

Garbled Serial Output

If the serial output appears to be garbled, missing characters, binary, or random characters check the following items:
Flow Control In some cases flow control can interfere with serial communication, causing dropped characters or other issues. Disabling flow control in the client can potentially correct this problem.
On PuTTY and other GUI clients there is typically a per-session option to disable flow control. In PuTTY, the Flow Control option is in the settings tree under Connection, then Serial.
To disable flow control in GNU Screen, add the -ixon and/or -ixoff parameters after the serial speed as in the following example:

```
$ sudo screen <console port> 115200,-ixon
```

- **Terminal Speed** Ensure the terminal program is configured for the correct speed. (See No Serial Output)
- **Character Encoding** Ensure the terminal program is configured for the proper character encoding, such as UTF-8 or Latin-1, depending on the operating system. (See GNU Screen)

Serial Output Stops After the BIOS
If serial output is shown for the BIOS but stops afterward, check the following items:

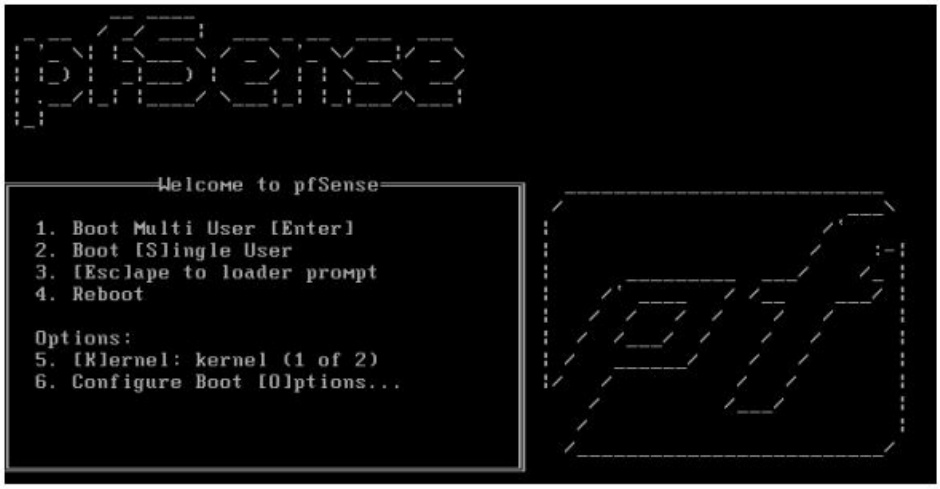
- **Terminal Speed** Ensure the terminal program is configured for the correct speed for the installed operating system.
  (See No Serial Output)
- **Device OS Serial Console Settings** Ensure the installed operating system is configured to activate the serial console and that it is configured for the proper console (e.g. ttyS1 in Linux). Consult the various operating install guides on this site for further information.
- **Bootable Media** If booting from a USB flash drive, ensure that the drive was written correctly and contains a bootable operating system image.

Reinstalling pfSense Plus Software

1. Please open a TAC ticket to request access to the Plus firmware by selecting Firmware Access as the General Problem and then select Netgate 4200 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-serial-23.09.1-RELEASE-amd64.img.gz
   Note: pfSense® Plus is preinstalled on Netgate appliances, which is optimally tuned for Netgate hardware and contains features that cannot be found elsewhere, such as ZFS Boot Environments, OpenVPN DCO, and the AWS VPC Wizard.
2. Write the image to a USB memstick.
   See also:
   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 the USB port on the right side and boot the system.
5. Wait for the BIOS prompt to appear.
6. Press Esc to enter the BIOS.
7. Use the left/right arrow keys to select the “Save & Exit” header.
8. Use the up/down arrow keys to move into the Boot Override section.
9. Select the entry for the USB memstick
   The entry is likely at or near the bottom of the list. The name of the entry varies by brand/make/model of the USB memstick.
10. 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.
11. Choose one of the console type options the installer offers for serial console installation.
    The optimal choice for a properly configured terminal is xterm. Choose the correct console output most compatible with the serial client.
    Note: Of the choices, vt100 is the most widely compatible type but it is also limited in how it can display output. The xterm option renders the best on GNU screen and many popular modern clients and terminals.
12. Read the Copyright and distribution notice displayed by the installer. Press Enter to accept the terms of the agreement.
13. The installer will automatically launch and present several options. On Netgate firewalls, choosing Enter for the

default options on each screen will complete the installation process. One exception to this is that it may be necessary to press the space bar to select the correct target disk.

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



See also:

For more information on the available choices during this process, see the Installation Walkthrough.

Tip: If there is an existing installation on this device, the Recover config.xml option will attempt to mount the existing installation drive and copy the previous configuration, including SSH keys. Choose that option first, then proceed through the install as usual.

14. If prompted to clean up multiple identical boot entries, select Yes and press the Enter key.
15. The installer will then prompt to Reboot. Select Reboot and press Enter. The device will shutdown and reboot.

```
Dec 21 22:41:37 Waiting (max 60 seconds) for system process `vnlru` to stop...␣
↪done
Waiting (max 60 seconds) for system process `syncer` to stop...
Waiting (max 60 seconds) for system process `bufdaemon` to stop... done
All buffers synced.
Uptime: 5m43s
umass0: detached
```

16. Remove the USB drive from the USB port.

    Important: If the USB drive remains attached, the system may boot into the installer again.

    See also:

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

    Caution: If this device contains multiple disks, such as when adding an SSD to an existing system which previously used MMC, additional steps may be necessary to ensure the device boots from and uses the correct disk. Furthermore, having separate installations of the software on different disks is a known source of problems.

    For example, the kernel could boot from one disk while the root filesystem is loaded from another, or they could contain conflicting ZFS pools.

    In some cases it is possible to adjust the BIOS boot order to prefer the new disk, but the best practice is to wipe the old disk to remove any chance of the previous installation causing boot issues or conflicts.

    For information on how to wipe the old disk, see Multiple Disk Boot Issues.

Configuring an OPT interface as an additional WAN

This guide configures an OPT port as an additionalWAN type interface. These interfaces connect to upstream networks providing connectivity to the Internet or other remote destinations.

See also:

Multi-WAN documentation

Configuring an additionalWAN

- Requirements
- Assign the Interface
- Interface Configuration
- Outbound NAT
- Firewall Rules
- Gateway Groups
- DNS
- Setup Policy Routing
- Dynamic DNS
- VPN Considerations
- Testing

Requirements

- This guide assumes the underlying interface is already present (e.g. physical port, VLAN, etc).
- The WAN configuration type and settings must be known before starting. For example, this might be an IP address, subnet mask, and gateway value for static addresses or credentials for PPPoE.

Assign the Interface

- Navigate to Interfaces > Assignments
  Look at list of current assignments. If the interface in question is already assigned, there is nothing to do. Skip ahead to the interface configuration.
- Pick an available interface in Available network ports
  If there are no available interfaces, then one may need to be setup in some other way (e.g. VLANs).
- Click Add
  The firewall will assign the next available OPT interface number corresponding to the internal interface designation.
  For example, if there are no current OPT interfaces, the new interface will be OPT1. The next will be OPT2, and so on.
  Note: As this guide does not know what that number will be on a given configuration, it will refer to the interface generically as OPTx.
  The newly assigned interface will have its own entry under the Interfaces menu and elsewhere in the GUI.

Interface Configuration
The new interface must be enabled and configured.

- Navigate to Interfaces > OPTx

- Check Enable interface
- Set custom name in the Description, e.g. WAN2
- Set IP address and CIDR for static, or DHCP/PPPoE/etc.

  See also:

  IPv4 Configuration Types
- Create a Gateway if this is a static IP address WAN:
  - Click Add a New Gateway
  - Configure the gateway as follows:
    - Default Check if this new WAN should be the default gateway.
    - Gateway Name Name it the same as the interface (e.g. WAN2), or a variation thereof.
    - Gateway IPv4 The IPv4 address of the gateway inside the same subnet.
    - Description Optional text describing the purpose of the gateway.
  - Click Add
  - Ensure the new gateway is selected as the IPv4 Upstream Gateway
- Check Block private networks

  This will block private network traffic on the interface, though if the firewall rules for this WAN are not permissive, this may be unnecessary.
- Check Block bogon networks

  This will traffic from bogus or unassigned networks on the interface, though if the firewall rules for this WAN are not permissive, this may be unnecessary.
- Click Save
- Click Apply Changes

The presence of a selected gateway in the interface configuration causes the firewall to treat the interface as a WAN type interface. This is manual for static configurations, as above, but is automatic for dynamic WANs (e.g. DHCP,PPPoE).
The firewall applies outbound NAT to traffic exiting WAN type interfaces but does not use WAN type interface networks as a source for outbound NAT on other interfaces. Firewall rules onWAN type interfaces get reply-to added to ensure traffic entering a WAN exits the same WAN, and traffic exiting the interface is nudged toward its gateway.
The DNS Resolver will not accept queries from clients on WAN type interfaces without manual ACL entries.
See also:
Interface Configuration

Outbound NAT
For clients on local interfaces to get to the Internet from private addresses to destinations through this WAN, the firewall must apply Outbound NAT on traffic leaving this new WAN.

- Navigate to Firewall > NAT, Outbound tab
- Check the current outbound NAT mode

  If the mode is set to Automatic or Hybrid, then this may not need further configuration. Ensure there are rules for the newWAN listed as a Interface in the Automatic Rules at the bottom of the page. If so, skip ahead to the next section.

  If the mode is set to Manual, create a new rule or set of rules to cover the new WAN.

If there are existing rules in the Mappings table, they can be copied and adjusted to use the new WAN. Otherwise, create them manually:

- Click

to add a new rule at the top of the list.
- Configure the rule as follows:
  - Interface Choose the new WAN interface (e.g. WAN2)
  - Address Family IPv4
  - Protocol Any
  - Source Network, and fill in the LAN subnet, e.g. 192.168.1.0/24.

    If there is more than one LAN subnet, create rules for each or use other methods such as aliases or CIDR summarization to cover them all.
  - Destination Any
  - Translation Address Interface Address
  - Description Text describing the rule, e.g. LAN outbound on WAN2
- Click Save
- Click Apply Changes

  Repeat as needed for additional LANs.

Firewall Rules

By default there are no rules on the new interface, so the firewall will block all traffic. This is ideal for a WAN, so is safe to leave as-is. Adding services on the new WAN, such as VPNs, may require rules but those should be handled on a case-by-case basis.

Warning: Do not add any blanket “allow all” style rules on any WAN.

Gateway Groups

Gateway Groups do not control traffic directly, but can be used in other places, such as firewall rules and service bindings, to influence how those areas use gateways.
For most scenarios it helps to create three gateway groups to start with: PreferWAN, PreferWAN2, and LoadBalance:

- Navigate to System > Routing, Gateway Groups tab
- Click Add to create a new gateway group
- Configure the group as follows:
  - Group Name PreferWAN
  - Gateway Priority Gateway for WAN on Tier 1, and WAN2 on Tier 2
  - Description Prefer WAN, fail to WAN2
- Click Save
- Click Add to create another gateway group
- Configure the group as follows:
  - Group Name PreferWAN2
  - Gateway Priority Gateway for WAN on Tier 2, and WAN2 on Tier 1
  - Description Prefer WAN2, fail to WAN

- Click Save
- Click Add to create another gateway group
- Configure the group as follows:
  - Group Name LoadBalance
  - Gateway Priority Gateways for WAN and WAN2 both on Tier 1
  - Description Prefer WAN2, fail to WAN
- Click Save
- Click Apply Changes

  Now set the default gateway to a failover group:
- Navigate to System > Routing, Gateways tab
- Set Default gateway IPv4 to PreferWAN
- Click Save
- Click Apply Changes

  Note: This is important for failover from the firewall itself so it always has outbound access. While this also enables basic failover for client traffic, it's better to use policy routing rules to control client traffic behavior.

DNS
DNS is critical for Internet access and it's important to ensure the firewall can always resolve hostnames using DNS even when running on a secondary WAN.
The needs here depend upon the configuration of the DNS Resolver or Forwarder.
If the DNS Resolver is in its default resolver mode, then default gateway switching will be sufficient to handle failover in most cases, though it may not be as reliable as using forwarding mode.
If the DNS Resolver is in forwarding mode or the firewall is using the DNS Forwarder instead, then maintaining functional DNS requires manually configuring gateways for forwarding DNS servers.

- Navigate to System > General Setup
- Add at least one DNS server for each WAN, ideally two or more

  These servers must be unique, the same server cannot be listed more than once.
- Select a gateway for each DNS server, corresponding to theWAN through which the firewall can reach the DNS server.

  For public DNS servers such as CloudFlare or Google, either WAN is OK, but if either WAN uses DNS servers from a specific ISP, ensure those exit the appropriate WAN.
- Uncheck DNS Server Override

  This will tell the firewall to use the DNS servers entered on this page and to ignore servers provided by dynamic WANs such as DHCP or PPPoE. Occasionally these providers may push conflicting DNS server information so the best practice is to assign the DNS servers manually.
- Click Save

Note: If the DNS Resolver has specific outgoing interfaces selected in its configuration, select the new WAN there well as well.

Setup Policy Routing

Policy routing involves setting a gateway on firewall rules which direct matching traffic out specific WANs or failover groups.
In simple cases (one LAN, no VPNs) the only requirement to configure policy routing is to add a gateway to

existing rules.

- Navigate to Firewall > Rules, LAN tab
- Edit the default pass rule for the LAN
- Click Display Advanced
  • Set the Gateway to one of the gateway groups based on the desired LAN client behavior.
  For example, pick PreferWAN so clients use WAN and then if WAN fails, they use WAN2.
- Click Save
- Click Apply Changes

If there are other local networks or VPNs which clients on LAN must reach, add rules above the default pass rules to pass local traffic without a gateway set:

- Navigate to Firewall > Rules, LAN tab
- Click

to add a new rule at the top of the list
- Configure the rule as follows:
  - Action Pass
  - Interface LAN
  - Protocol Any
  - Source LAN net
  - Destination The other local subnet, VPN network, or an alias of such networks.
  - Description Pass to local and VPN networks
    Do not set a gateway on this rule.
- Click Save
- Click Apply Changes

Dynamic DNS
Dynamic DNS provides several benefits for multiple WANs, particularly with VPNs. If the firewall does not already have one or more Dynamic DNS hostnames configured, consider signing up with a provider and creating one or more.
It's a good practice to have a separate DNS entry for each WAN and a shared entry for failover, or one per failover group. If that is not viable, at least have one for the most common needs.
The particulars of configuring Dynamic DNS entries vary by provider and are beyond the scope of this document.

VPN Considerations
IPsec can use a gateway group as an as interface, but needs a dynamic DNS hostname as companion. The remote peer would need to use the Dynamic DNS hostname as the peer address of this firewall instead of an IP address. Because this relies on DNS, failover can be slow.
WireGuard does not bind to an interface, but can work with Multi-WAN. It will respond fromWAN2 if client contacts WAN2, but when initiating it will always use the current default gateway. Static routes can nudge traffic for a specific peer out a specific WAN.
OpenVPN can use a gateway group as an interface for clients or servers. Client behavior is OK and should match default failover behavior configured on the group. For servers it is better to bind the server to localhost and use port forwards from each WAN to localhost. Remote clients can then have multiple remote entries and contact each WAN as needed at any time.

Testing
Methods for testing depend on the type of WANs and gateway groups in use.

- For most WANs, a better test is to unplug the upstream connection from the CPE. This more accurately simulates a typical type of upstream connectivity failure. Do not power off the CPE or unplug the connection between the firewall and the CPE. While this may work, it's a much less common scenario and can behave differently.
- For testing load balancing, use cURL or multiple browsers/sessions when checking the IP address multiple times. Refreshing the same browser window will reuse a connection to the server and is not helpful for testing connection-based load balancing.

Configuring an OPT interface as an additional LAN

This guide configures an OPT port as an additional LAN type interface. These local interfaces can perform a variety of tasks, such as being a guest network, DMZ, IOT isolation, wireless segment, lab network, and more.

Configuring an additional LAN

- Requirements
- Assign the Interface
- Interface Configuration
- DHCP Server
- Outbound NAT
- Firewall Rules
  - Open
  - Isolated
- Other Services

Requirements

- This guide assumes the underlying interface is already present (e.g. physical port, VLAN, etc).
- Choose a new local subnet to use for the additional LAN type interface. This example uses 192.168.2.0/24.

Assign the Interface

The first step is to assign an OPT interface.

- Navigate to Interfaces > Assignments
  Look at list of current assignments. If the interface in question is already assigned, there is nothing to do. Skip ahead to the interface configuration.
- Pick an available interface in Available network ports
  If there are no available interfaces, then one may need to be setup in some other way (e.g. VLANs).
- Click Add
  The firewall will assign the next available OPT interface number corresponding to the internal interface designation.
  For example, if there are no current OPT interfaces, the new interface will be OPT1. The next will be OPT2, and so on.

Note: As this guide does not know what that number will be on a given configuration, it will refer to the interface generically as OPTx.
The newly assigned interface will have its own entry under the Interfaces menu and elsewhere in the GUI.

Interface Configuration
The new interface must be enabled and configured.

- Navigate to Interfaces > OPTx
- Check Enable interface
- Set custom name in the Description, e.g. GUESTS, DMZ, etc.
- Set the IP address and CIDR mask for the new LAN

  For this example, 192.168.2.1/24.
- Do not add or choose a gateway
- Uncheck Block private networks

  This interface is a private network, this option would prevent it from functioning.
- Uncheck Block bogon networks

  The rules on this interface should only allow traffic from the subnet on the interface, making this option unnecessary.
- Click Save
- Click Apply Changes

The lack of a selected gateway in the interface configuration causes the firewall to treat the interface as a LAN type interface.
The firewall uses LAN type interfaces as sources of outbound NAT traffic but does not apply outbound NAT on traffic exiting a LAN. The firewall does not add any extra properties on firewall rules to influence traffic behavior.
The DNS
Resolver will accept queries from clients on LAN type interfaces.
See also:
Interface Configuration

DHCP Server
Next, configure DHCP service for this local interface. This is a convenient and easy way assign addresses for clients on the interface, but is optional if clients will be statically addressed instead.

- Navigate to Services > DHCP Server, OPTx tab (Or the custom name)
- Check Enable
- Configure the Range, e.g. from 192.168.2.100 to 192.168.2.199

  This sets the lower (From) and upper (To) bound of automatic addresses assigned to clients.
- The rest can be left at defaults
- Click Save

See also:
DHCPv4 Configuration

Outbound NAT
For clients on this interface to get to the Internet from private addresses, the firewall must apply Outbound NAT for the new subnet.

- Navigate to Firewall > NAT, Outbound tab

- Check the current outbound NAT mode

  If the mode is set to Automatic or Hybrid, then this may not need further configuration. Ensure the new LAN subnet is listed as a Source in the Automatic Rules at the bottom of the page. If so, skip ahead to the next section to configure Firewall Rules.

  If the mode is set to Manual, create a new rule or set of rules to cover the new subnet.
- Click

to add a new rule at the top of the list
- Configure the rule as follows:
  - Interface Choose the WAN interface. If there is more than one WAN interface, add separate rules for each WAN interface.
  - Address Family IPv4
  - Protocol Any
  - Source Network, and fill in the new LAN subnet, e.g. 192.168.2.0/24.
  - Destination Any
  - Translation Address Interface Address
  - Description Text describing the rule, e.g. Guest LAN outbound on WAN
- Click Save
- Click Apply Changes

  Alternately, clone existing NAT rules and adjust as needed to match the new LAN.

Firewall Rules
By default there are no rules on the new interface, so the firewall will block all traffic. This is not ideal for a LAN as generally speaking, the LAN clients will need to contact hosts through the firewall.
Rules for this interface can be found under Firewall > Rules, on the OPTx tab (or the custom name, e.g. GUESTS).
There are two common scenarios administrators typically choose for local interfaces: Open and Isolated

Open
On an open LAN, hosts in that LAN are free to contact any other host through the firewall. This might be a host on the Internet, across a VPN, or on another local LAN.

In this case a simple “allow all” style rule for the interface will suffice.

- Navigate to Firewall > Rules, on the OPTx tab (or the custom name)
- Click

to add a new rule at the top of the list
- Configure the rule as follows:
  - Action Pass
  - Interface OPTx (or the custom name) should already be set by default
  - Protocol Any
  - Source OPTx Net (or the custom name)
  - Destination Any
  - Description Text describing the rule, e.g. Default allow all from OTPx
- Click Save
- Click Apply Changes
- Add rule to pass any protocol from interface net to any destination

Isolated
In an isolated local network, hosts on the network cannot contact hosts on other networks unless explicitly allowed in the rules. Hosts can still contact the Internet as needed in this example, but that can also be restricted by more complicated rules.
This scenario is common for locked down networks such as for IOT devices, a DMZ with public services, untrusted Guest/BYOD networks, and other similar scenarios.

Warning: Do not rely on tricks such as using policy routing to isolate clients. A full set of reject rules as described in this example are the best practice.

Create RFC1918 alias or alias containing at least the local/private networks on this firewall, such as VPNs. Using all of the RFC1918 networks is a safer practice

- Navigate to Firewall > Aliases
- Click Add
- Configure it as follows:
  - Name PrivateNets
  - Description Private Networks
  - Type Network(s)
- Add entries for:
  - 192.168.0.0/16
  - 172.16.0.0/12
  - 10.0.0.0/8
- Click Save
- Navigate to Firewall > Rules, on the OPTx tab (or the custom name)

  Add rule to pass DNS to firewall (or other DNS servers)
- Click to add a new rule at the bottom of the list.
- Configure the rule as follows:
  - Action Pass
  - Interface OPTx (or the custom name)
  - Protocol TCP/UDP
  - Source OPTx Net (or the custom name)
  - Destination This Firewall (self)

    If clients are to use DNS servers other than the firewall, use those as the destination instead.
  - Destination Port Range DNS, or choose Other and enter 53

    To allow DNS over TLS as well, add another rule for DNS over TLS or port 853.
  - Description Text describing the rule, e.g. Allow clients to resolve DNS through the firewall
- Click Save

  Add rule to pass ICMP to firewall
- Click to add a new rule at the bottom of the list.
- Configure the rule as follows:
  - Action Pass
  - Interface OPTx (or the custom name)
  - Protocol ICMP

    - ICMP Subtype Any is OK in this case, ICMP is useful but some people prefer to limit to Echo
    - Request only to allow ping and nothing else.
    - Source OPTx Net (or the custom name)
    - Destination This Firewall (self)
    - Description Allow client ICMP to the firewall
- Click Save

Add rule to reject any other traffic to firewall

- Click

to add a new rule at the bottom of the list.
- Configure the rule as follows:
    - Action Reject
    - Interface OPTx (or the custom name)
    - Protocol Any
    - Source Any
    - Destination This Firewall (self)
    - Description Reject all other traffic to the firewall
- Click Save

Add rule to reject traffic from this network to private networks

    - Click

to add a new rule at the bottom of the list.
- Configure the rule as follows:
    - Action Reject
    - Interface OPTx (or the custom name)
    - Protocol Any
    - Source Any
    - Destination Single Host or Alias, PrivateNets (the alias created earlier)
    - Description Reject all other traffic to private networks
- Click Save

  Add rule to pass from this interface network to any destination:
- Click

to add a new rule at the bottom of the list.
- Configure the rule as follows:
    - Action Pass
    - Interface OPTx (or the custom name)
    - Protocol Any
    - Source OPTx Net (or the custom name)
    - Destination Any
    - Description Default allow all from OTPx
- Click Save

With the rules all in place, now click Apply Changes to finish and activate the new rules.
After the configuration, the rules should look like the following figure:

Fig. 5: Example firewall rules for isolated LAN type segment

Tip: Rule separators are useful for documenting a ruleset in place.
Similar to the isolated network, it's also possible to be much more strict with rules to only allow specific outbound ports. When creating this type of configuration,

Other Services
In most cases the above configuration is sufficient and clients on the new LAN can now obtain an address and get out to the Internet. However, there may be other custom settings which need accounted for when adding a new local interface:

- If the DNS resolver has specific interface bindings, add the new interface to the list.
- If using ALTQ traffic shaping, re-run the shaper wizard to include this new LAN type interface.
- Consider using captive portal to control access the interface

Factory Reset Procedure

This procedure performs a factory reset using the hardware reset button on the Netgate 4200. This button is located on the rear side of the unit toward the left end, between the power and console connectors and under the power button.
See Input and Output Ports for reference photos.
See also:

- Factory Reset from GUI or Console

Unlike some other models of Netgate hardware, the reset procedure on Netgate 4200 can be triggered while the device is running and does not require complicated timing.

1. Power on the device if it is not already running.
   If the device is booting, wait for the Diamond LED to start flashing blue or turn solid blue.
2. Press and hold the reset button (bottom).
   Note: This is the bottom (recessed) button and may require a pen, paperclip, or similar tool to press.
   The LEDs will start to fill in red one by one (Circle, Square, then Diamond) while the button is held in the depressed state.
3. Continue holding in the button until all of the LEDs start flashing red.
   This will take approximately 8 seconds. One the LEDs start flashing red, the factory reset is in progress and the button can be released. The device will reboot automatically.
   To cancel the reset procedure, release the button at any point before the LEDs begin to flash red. The Diamond

LED will return to a solid blue state indicating that the reset has been canceled.

4. Wait for the system to complete the reset and finish the boot process.

   At the end of the boot process the LEDs will return to the ready state, with the Diamond LED solid blue.

When the device boots again it will be at its factory default settings and accessible from the LAN at **https://192.168.1.1**.
If this procedure fails, connect to the console and perform a factory reset there.

Additional Resources

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

Resource Library
To learn more about how to use Netgate appliances and for other helpful resources, make sure to browse the Netgate Resource Library.
https://www.netgate.com/resources

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

Community Options
Customers who elected not to get a paid support plan, can find help from the active and knowledgeable pfSense software community on the Netgate forum.
https://forum.netgate.com/

Warranty and Support

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

For support information, view support plans offered by Netgate.

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

Documents / Resources

	Netgate 4200 Security Gateway [pdf] User Manual 4200 Security Gateway, 4200, Security Gateway, Gateway

References

- American Arbitration Association | ADR.org
- Backup and Recovery — Using the AutoConfigBackup Service | pfSense Documentation
- Configuration — Console Menu Basics | pfSense Documentation
- Installing and Upgrading — Perform the Installation — Installation Walkthrough | pfSense Documentation
- Installing and Upgrading — Upgrade Guide | pfSense Documentation
- Packages — AWS VPC Wizard | pfSense Documentation
- Troubleshooting — Troubleshooting Multiple Disks | pfSense Documentation
- Home | Netgate Forum
- TAC Support Request
- Netgate 4200 pfSense+ Software - VPN, Routing, & Firewall Security Gateway Appliance
- Professional Services
- Resources Library
- Netgate Global Support
- Product Lifecycle
- Netgate® Training and Certification
- CP210x USB to UART Bridge VCP Drivers - Silicon Labs
- SecureCRT - The rock-solid Telnet and SSH client for Windows, Mac, and Linux
- User Manual

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.