netgate

Security Gateway Manual

Netgate-4100

© Copyright 2026 Rubicon Communications LLC

Feb 06, 2026

CONTENTS

This Quick Start Guide covers the first time connection procedures for the Netgate® 4100 Desktop Firewall Appliance and will provide the information needed to keep the appliance up and running.

OUT OF THE BOX

1.1 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 Customer Premise Equipment (CPE) device, such as a cable or fiber router. 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.
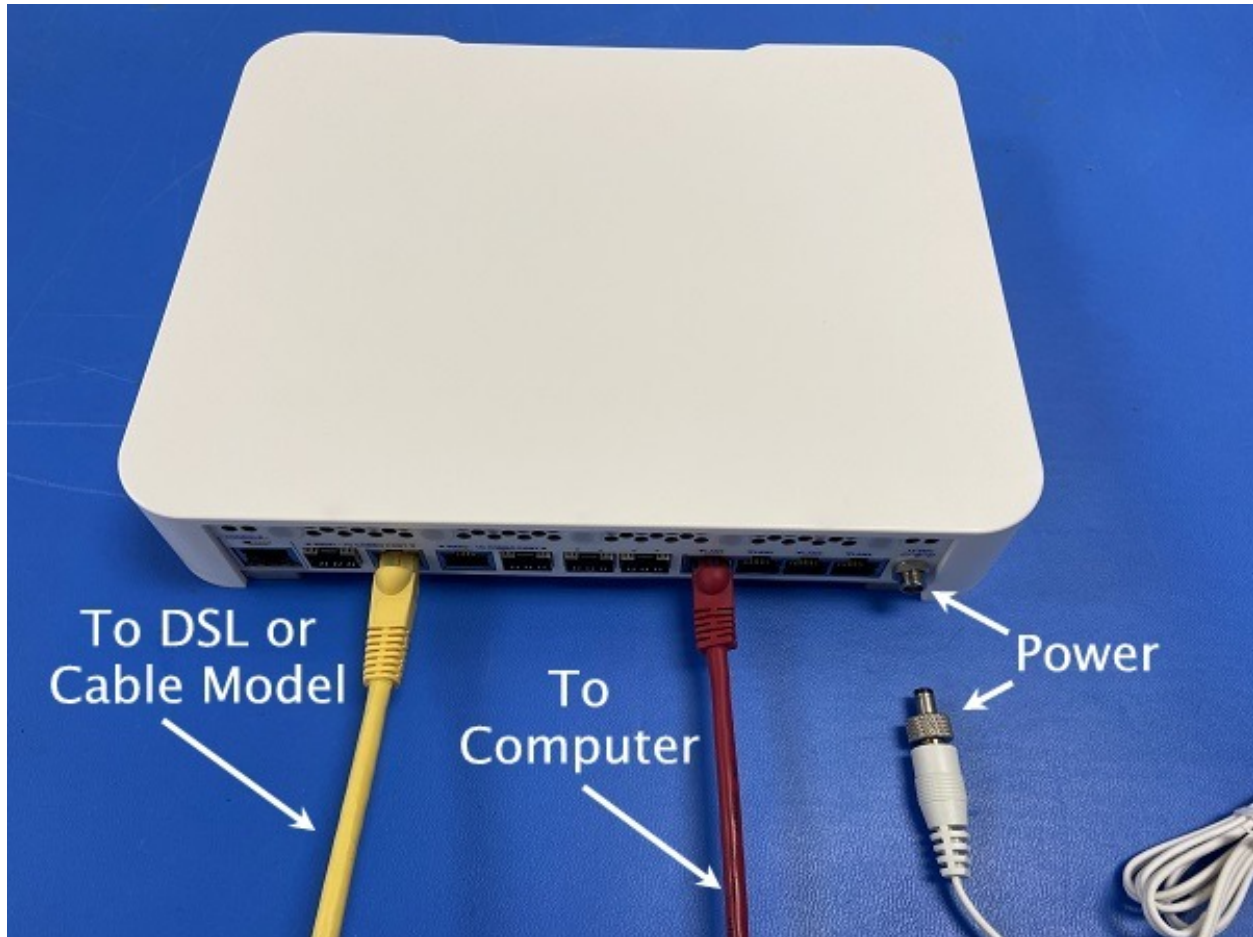
1.1.1 What next?

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*.

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 the WAN** 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.

1.2 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 ISP Customer Premise Equipment (CPE) on WAN (e.g. Fiber or Cable Router) has a default IP Address of `192.168.1.1`, disconnect the Ethernet cable from the WAN1 port on the Netgate 4100 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.

1.2.1 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`.
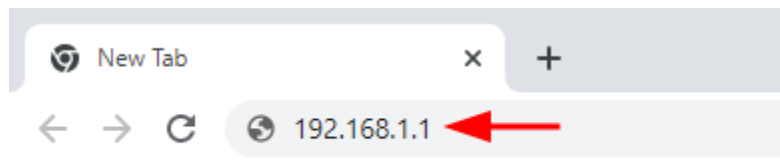

Fig. 1: Enter the default LAN IP address in the browser

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`

1.2.2 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.

Your connection is not private

Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

Hide advanced ← ①

Back to safety

This server could not prove that it is **192.168.1.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.1 (unsafe) ← ②

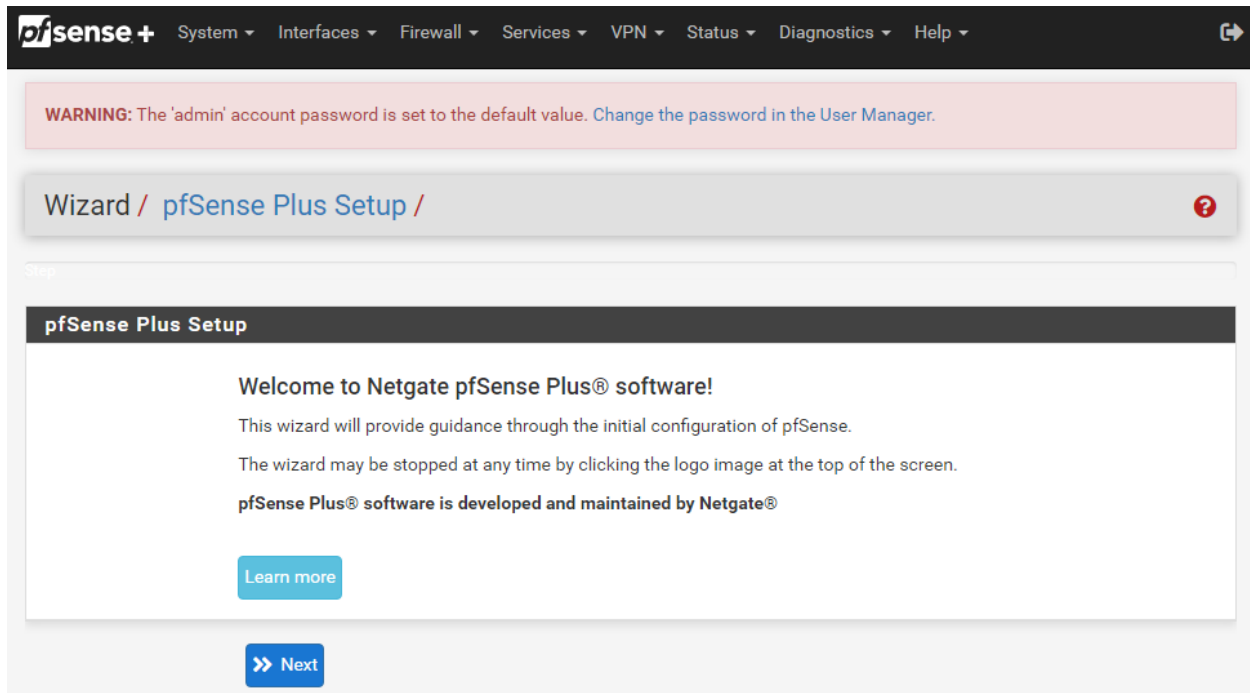Fig. 2: Example certificate warning message

Fig. 3: Setup Wizard starting page

1. Click **Next** to start the **Setup Wizard**.

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.
    > ---

    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.

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

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

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

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**.

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 WAN1 port on the Netgate 4100 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.

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

1.2.3 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 WAN1 port now.

This completes the basic configuration for the Netgate appliance.

Copyright and Trademark Notices.

Copyright© 2004-2016. Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved.
Copyright© 2014-2023. 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.

Accept

Fig. 7: Copyright and Trademark Notices

1.3 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.

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.
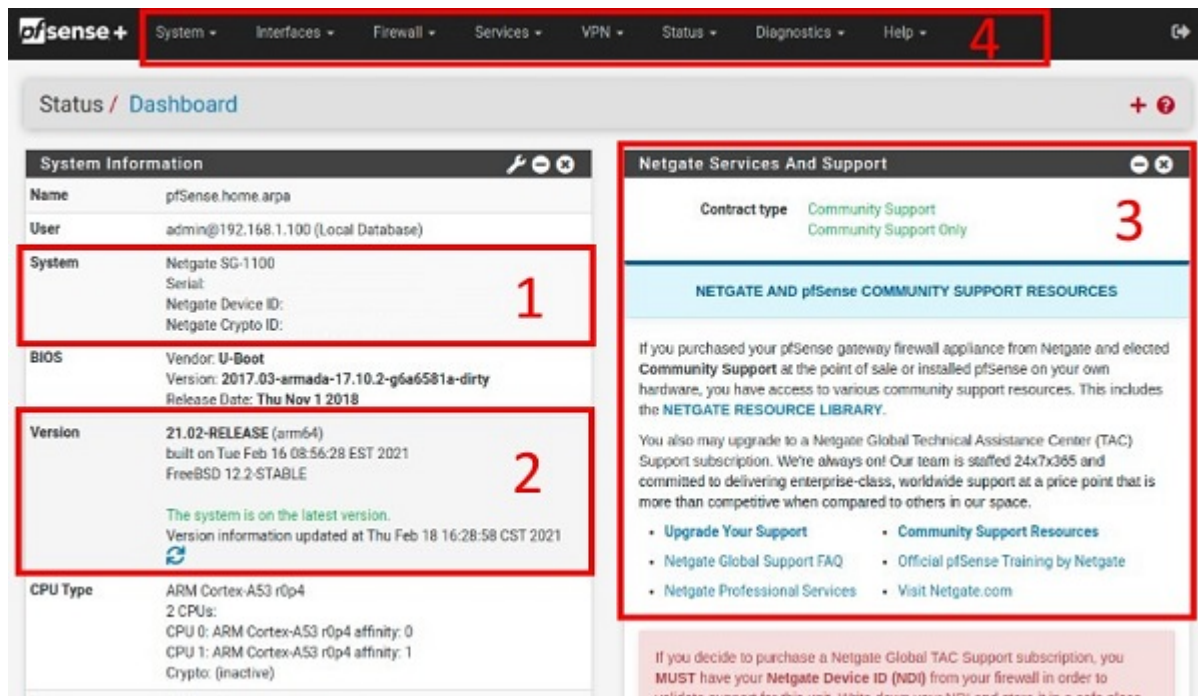
Fig. 8: The pfSense® Plus Dashboard

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.

1.3.2 Re-running the Setup Wizard

To re-run the Setup Wizard, navigate to **System > Setup Wizard**.
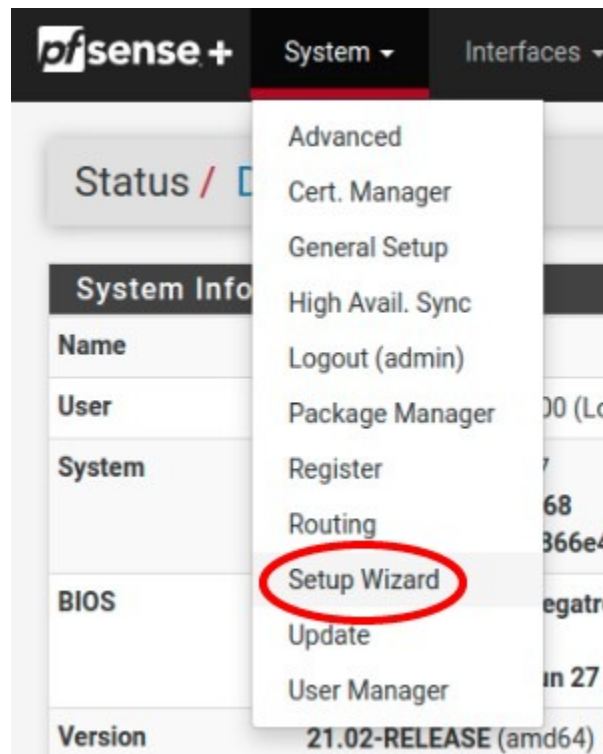
Fig. 9: Re-run the Setup Wizard

1.3.3 Backup and Restore

It is important to back up 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.
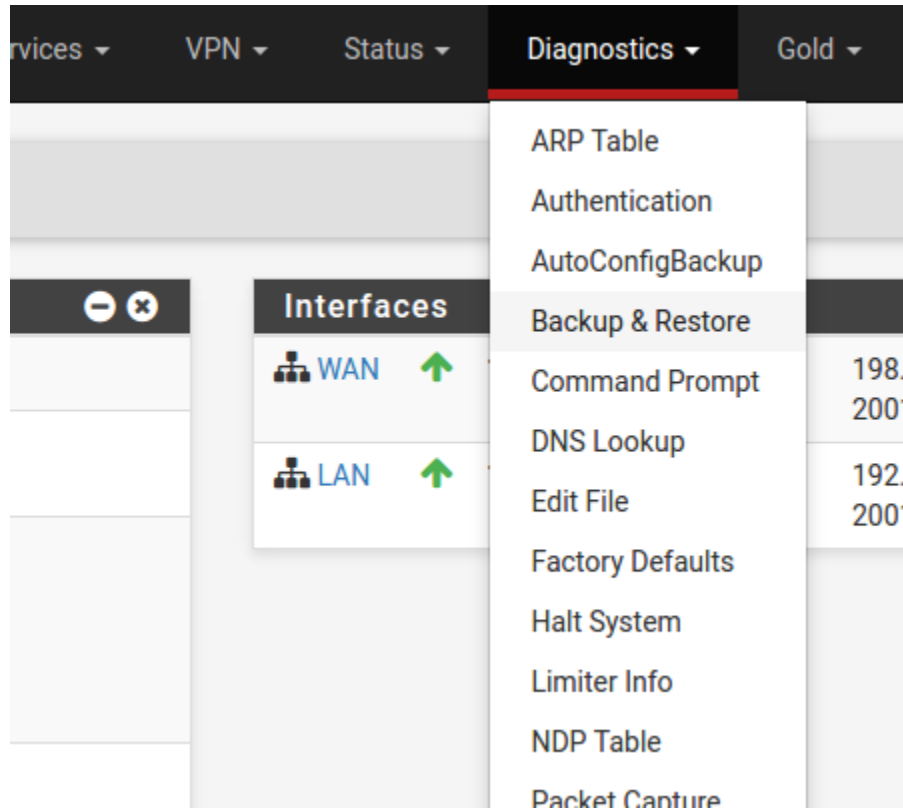
Fig. 10: Backup & Restore
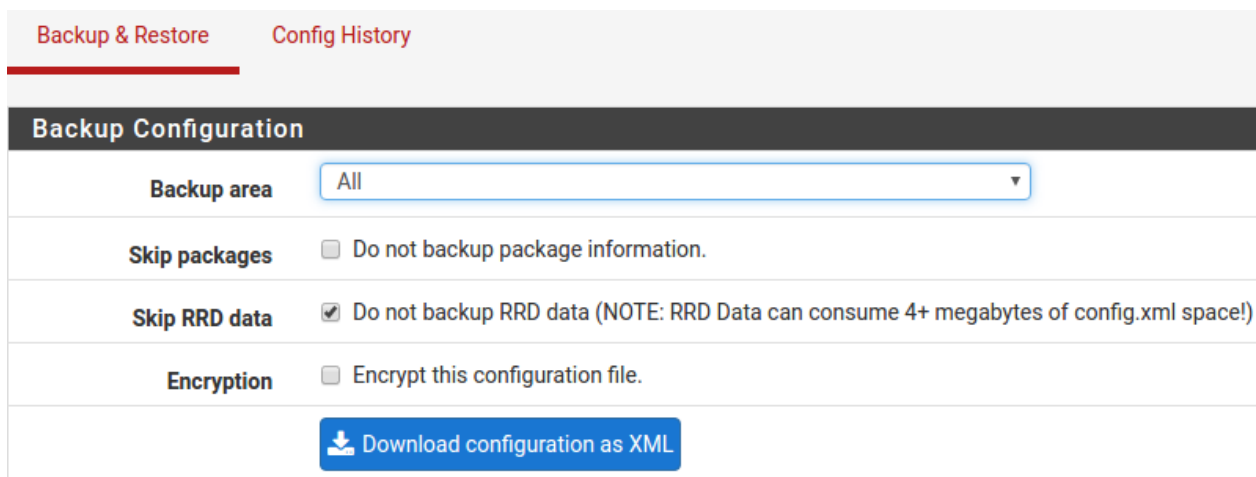
Fig. 11: Click Download configuration as XML

1.3.4 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. 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.

1.3.5 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 perform 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.

1.4 Input and Output Ports
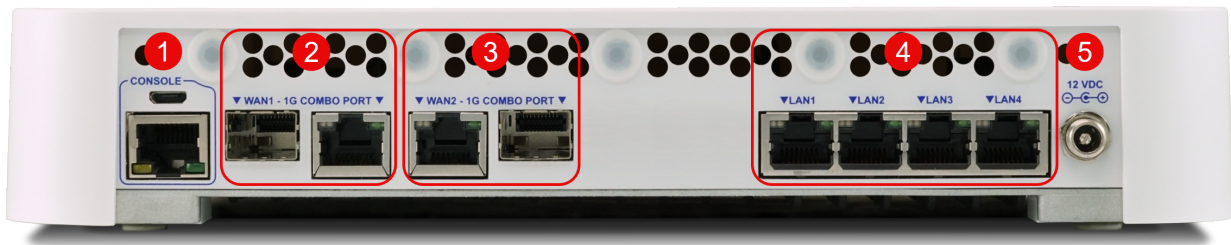
Fig. 12: Rear side view of the Netgate 4100 Firewall Appliance
The numbered labels in this image refer to entries in *Networking Ports* and *Non-Networking Ports*.

1.4.1 Non-Networking Ports

Port	Description
1	Serial Console (*USB* or *RJ45*)
5	Power

- 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.

- The Power connector is 12VDC with threaded locking connector. Power Consumption 20W (idle)

1.4.2 Networking Ports

The WAN1 and WAN2 Combo-Ports are shared ports. Each has an RJ-45 port and an SFP port. Only the RJ-45 *or* the SFP connector can be used each port.

Note: Each port, WAN1 and WAN2, is discrete and individual. It is possible to use the RJ-45 connector on one port and the SFP connector on the other.

Port	Interface Name	Port Name	Port Type	Port Speed
2	WAN1	ix3	RJ-45/SFP	1 Gbps
3	WAN2	ix2	RJ-45/SFP	1 Gbps
4	LAN1 - LAN4	igc0 - 3	RJ-45	2.5 Gbps

Note: The default configuration has all ports assigned as WANs and LANs to match the labels on the back of the device. These are only pre-defined labels; any port can be renamed and configured for any purpose.

Note: The `igc(4)` and `ix(4)` network interfaces on this device **do not** implement 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.

1.4.3 Front Side

Fig. 13: Front view of the Netgate 4100 Firewall Appliance

LED Patterns

Description	LED Pattern
Standby	Circle solid orange
Power On	Circle solid blue
Boot in Process	All rapidly flash blue
Boot Completed/Ready	Diamond slowly flashes blue
Upgrade Available	Square slowly flashes orange
Upgrade in Progress	All rapidly flash green
Waiting to Reset	All solid red (*Factory Reset Procedure*)
Reset Confirmed	All rapidly flash red (*Factory Reset Procedure*)

1.4.4 Left Side

Fig. 14: Left side view of the Netgate 4100 Firewall Appliance

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

#	Description	Purpose
1	Reset Button (Recessed)	Used when performing a *Factory Reset Procedure*.
2	Power Button (Protruding)	Graceful shutdown (Hold 5s), hard power off (15s), power on (1s)
3	2x USB 3.0 Ports	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 implemented by add-on packages. For example, UPS/Battery Backups, Cellular modems, GPS units, and storage devices. Though the operating system also includes drivers for wired and wireless USB network devices, these are not ideal and should be avoided.

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.

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.

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 an 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.

Deutsch

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist, nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

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 prohla uje, e tento NETGATE device, je ve shod se základními po adavky a dal ími p íslu n mi ustanoveními sm rnice 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)

ΕλληνιχΗ [Greek]

ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGATE ΔΗΛΩΝΕΙ ΟΤΙ NETGATE device, ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙ-ΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1995/5/ΕΚ.

Magyar [Hungarian]

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

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 įrenginys 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.

Slovensky [Slovak]

NETGATE t mto vyhlasuje, e NETGATE device, sp a základné po iadavky a v etky príslu né ustanovenia Smernice 1999/5/ES.

Svenska [Swedish]

Härmed intygar NETGATE att denna NETGATE device, står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Español [Spanish]

Por medio de la presente NETGATE declara que el NETGATE device, cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

Polski [Polish]

Niniejszym, firma NETGATE o wiadcza, e produkt serii NETGATE device, spełnia zasadnicze wymagania i inne istotne postanowienia Dyrektywy 1999/5/EC.

Português [Portuguese]

NETGATE declara que este NETGATE device, está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

Română [Romanian]

Prin prezenta, NETGATE declară că acest dispozitiv NETGATE este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/CE.

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
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.

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 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

2.1 Netgate 4100 Rack Mount

The Netgate 4100 has an optional Rack Mount Kit available. This page provides an overview for attaching the system to the rack mount.

Fig. 1: The Netgate 4100 Rack Mounted

Note: The Rack Mount Kit is identical for the Netgate 4100, the Netgate 6100, and the Netgate 8200.

The Netgate 4100 Rack Mount Kit contains all the components necessary to mount the Netgate 4100.

2.1.1 The kit contains:

- 1 Anodized Rack Chassis
- 1 Rack Faceplate
- 1 USB 3.0 panel mount cable (pre-attached to the faceplate)
- 1 M3 Phillips flat head thread rolling screw
- 4 M4 x 40mm Socket Head Cap Screws (Hex / Allen drive)
- 2 Long Cable Ties (11.5")
- 2 Short Cable Ties (3")

Note: The Kit does not include the Netgate 4100, nor does it include the AC/DC Power Supply Brick.

Fig. 2: The Netgate 4100 Rack Mount Kit

2.1.2 Tools required:

- #1 Philips Screwdriver
- 3mm Hex Key (Allen) Wrench

2.1.3 Rack Mount Assembly Instructions

1. Insert the tabs on the right edge of the faceplate with the two slots in the right front corner of the rack mount chassis.
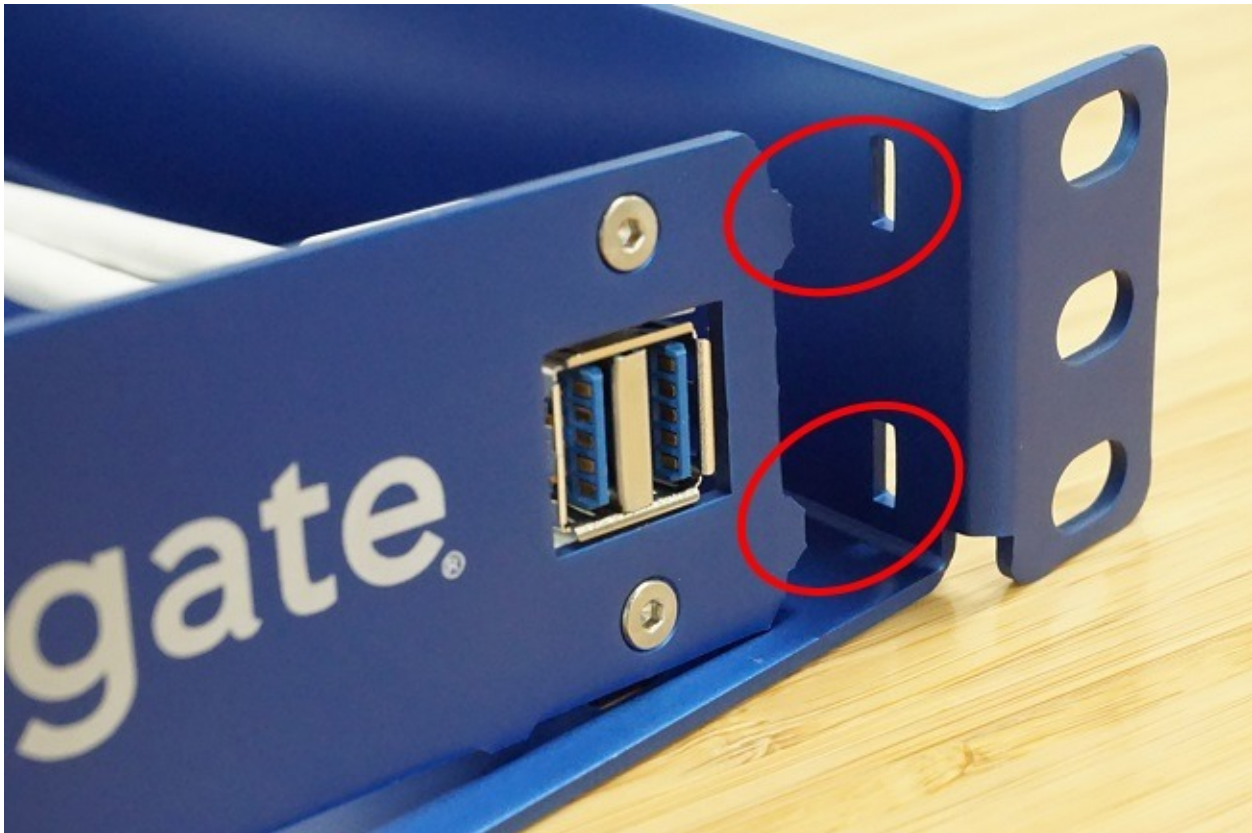

Fig. 3: Line up and Insert the Tabs to the Slots on the Right

2. Align the tabs on the bottom edge of the faceplate and insert into the two slots in the bottom of the chassis.

3. Using a Philips screwdriver, gently thread the screw until the screw is fully inserted, and the head stops flush with the faceplate.

> **Warning:** Do not overtighten.

4. If converting a desktop appliance to a rack mount system, remove the rubber feet from the bottom of the desktop unit.

> **Note:** It is important to remove the feet, especially for racking something in the slot directly below the Netgate
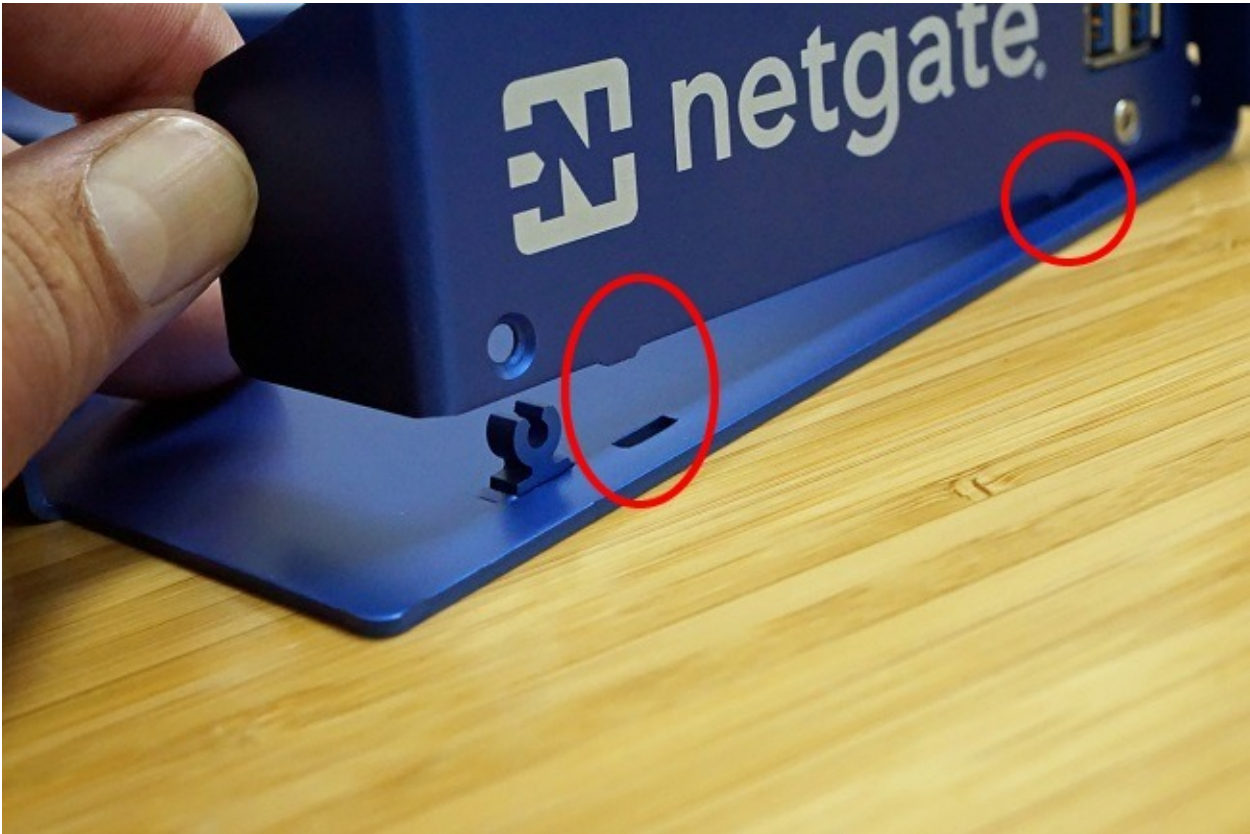
Fig. 4: Line up and Insert the Tabs to the Slots on the bottom

Fig. 5: Insert the Screw

appliance.

Fig. 6: Remove the Rubber Feet

5. With the rubber feet removed, line up the mounting holes in the system housing with the mounting tabs on the rack mount.

Note: The LEDs face the rear, the ports face the front, as shown. The system cannot be reversed without potential damage to the appliance.

6. Insert the M4 x 40mm socket head cap screws into the tabs and mounting holes. Using a 3mm hex key, gently tighten the M4 socket head screws.

Warning: Do not overtighten.

7. Place 1 large cable tie through each of the large holes in the chassis.

8. Place the power supply as shown and tighten the cable ties. Also add the small 3" cable tie as shown in the picture.
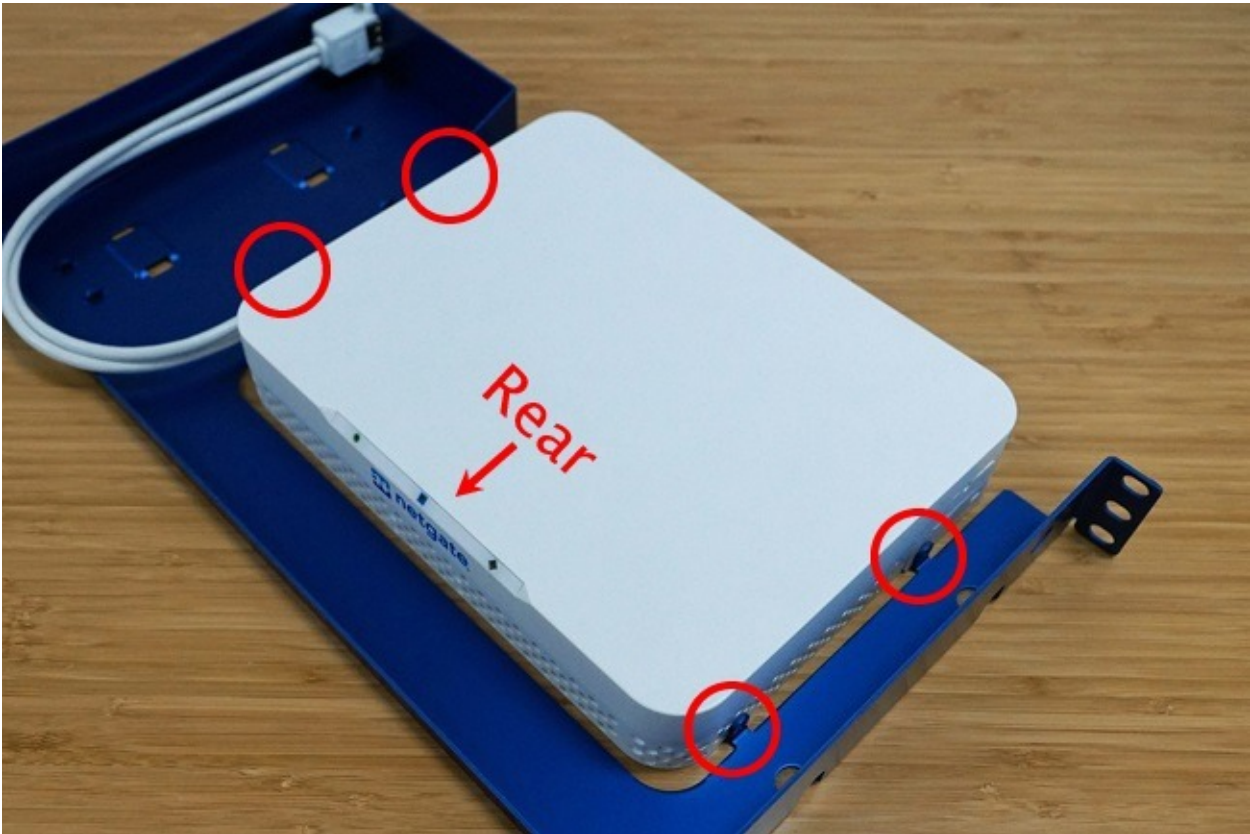
Fig. 7: Appliance Lined up with the Rack Mount
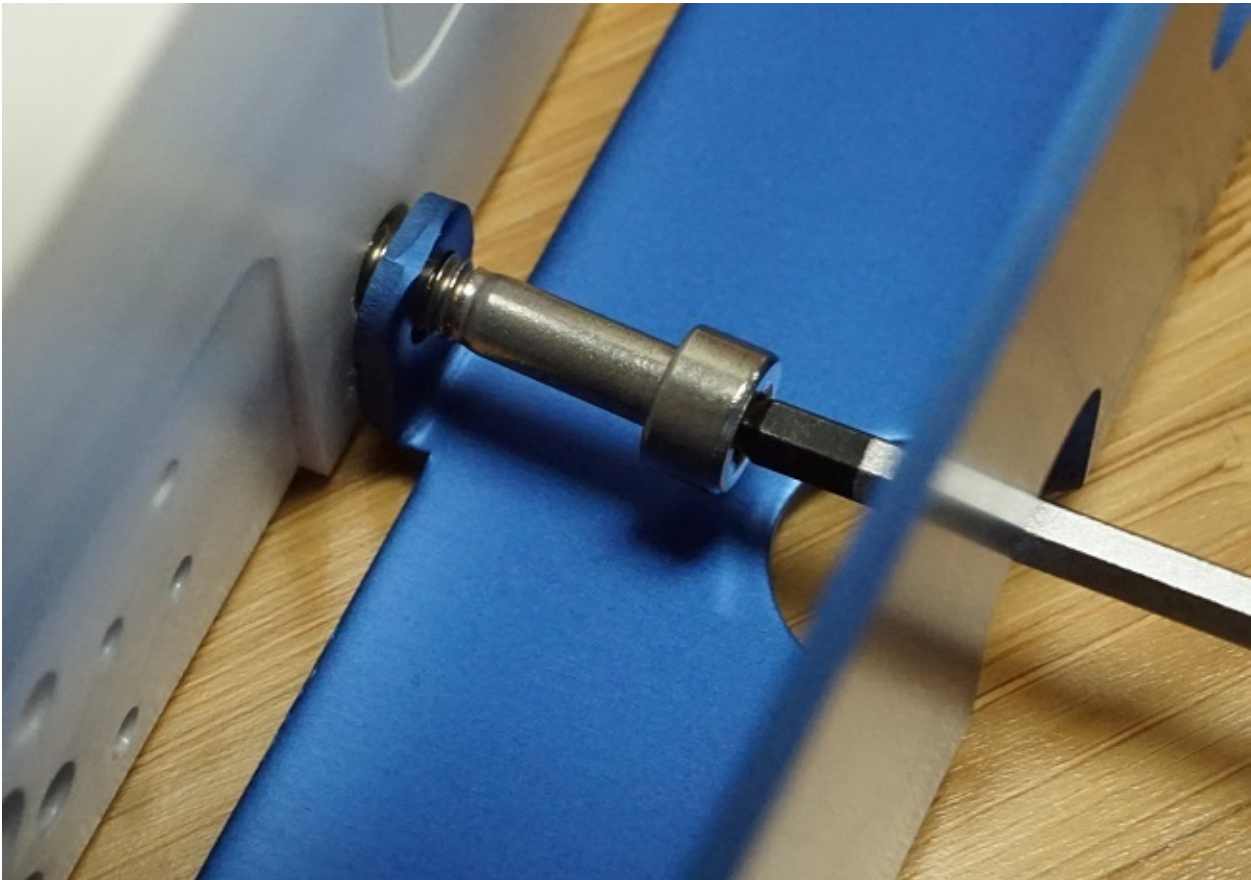
Fig. 8: Close-up of Alignment

Fig. 9: Repeat for all Four Mounting Holes
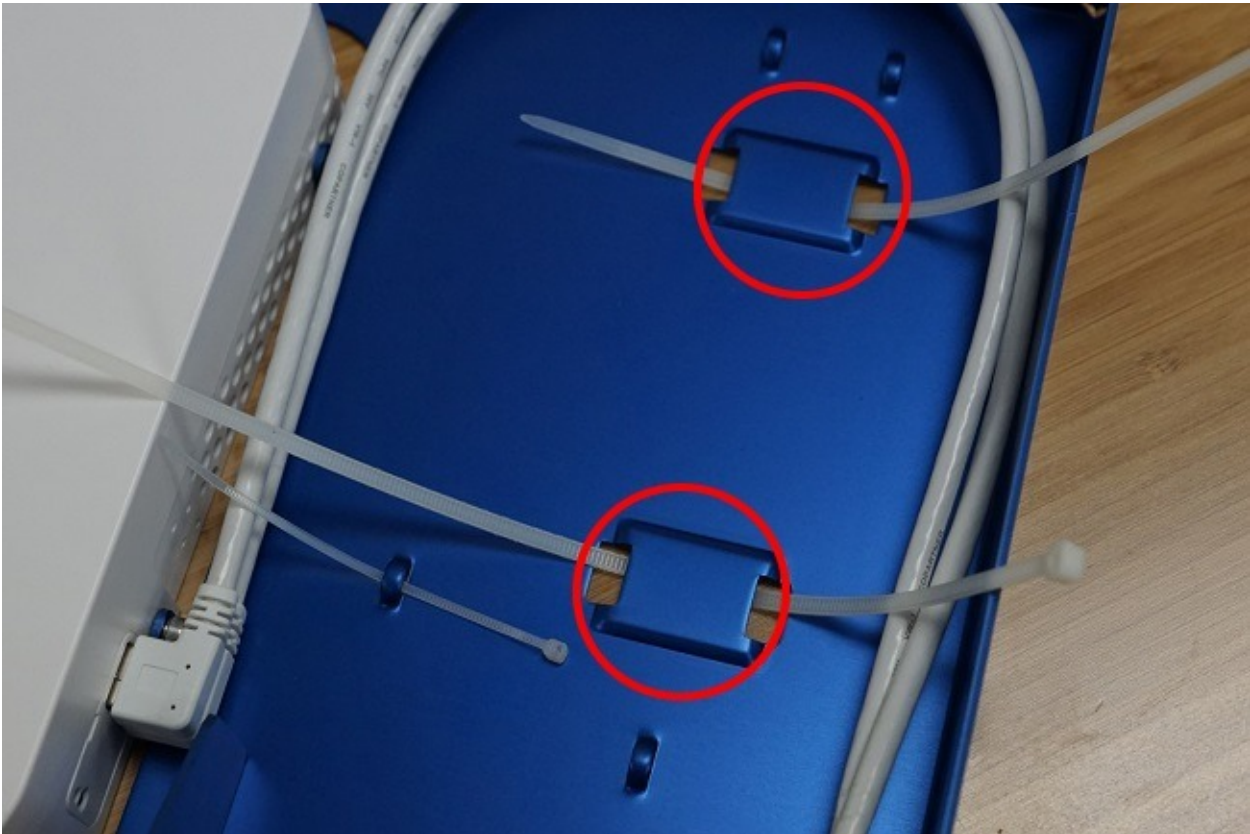
Fig. 10: Insert 11.5" Cable Ties
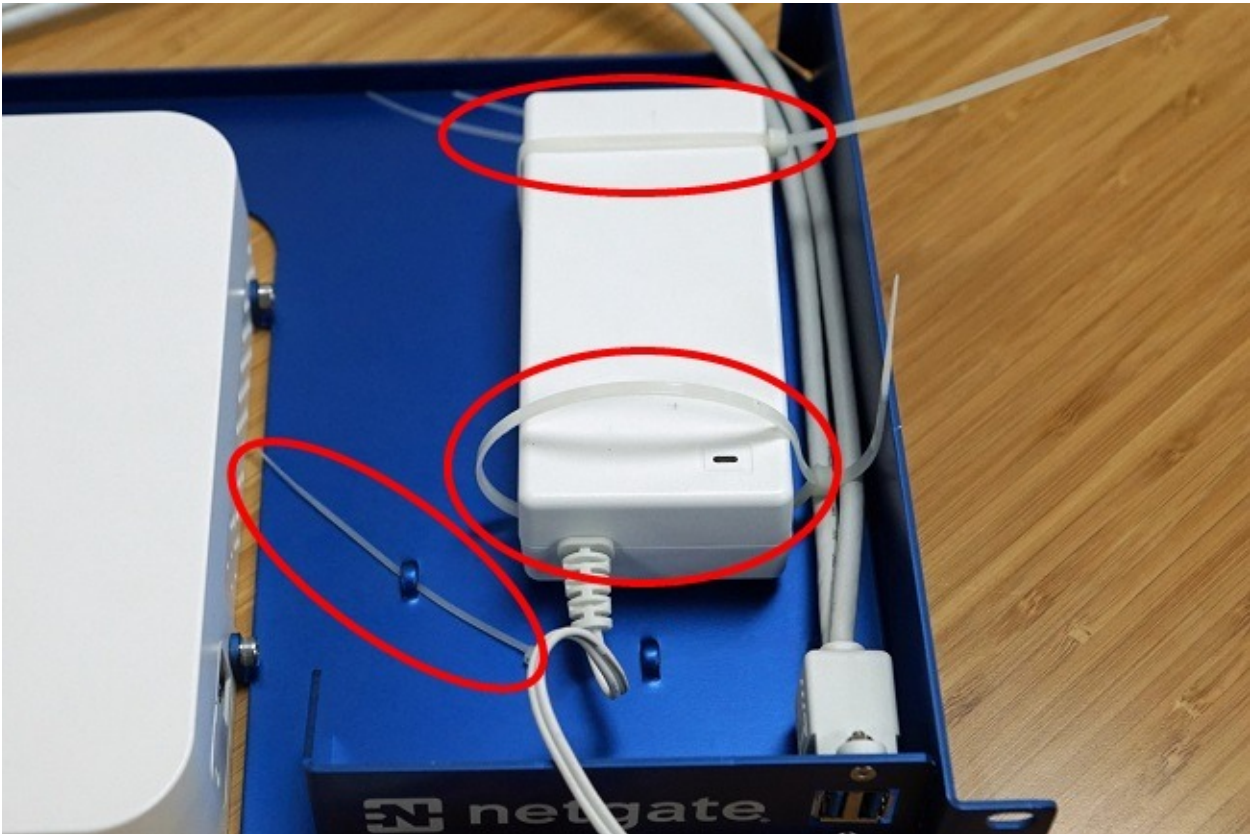
Fig. 11: Tighten the Cable Ties. Add the Small Cable Tie as Shown.

9. Using a small cable tie, loosely fasten the bundle of Power Supply output wires to the chassis as shown below.
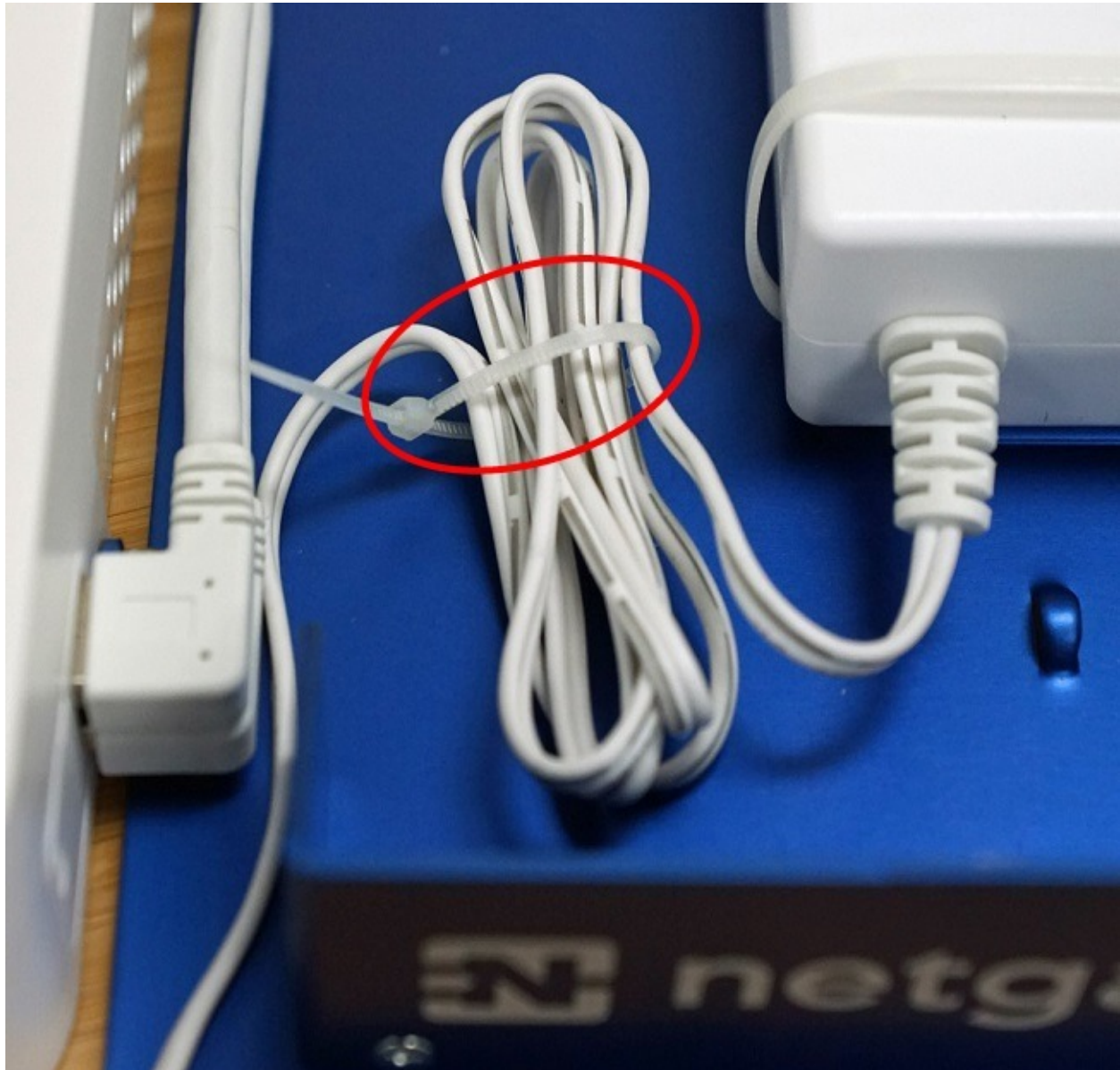
Fig. 12: Do not Cinch Down the Cable Tie Yet

10. Connect the power input jack on the front of the system and adjust the length of the power wire to remove any tension.

11. Pull the cable ties tightly around the power supply and the wire bundle. Cut the cable ties.

12. Plug in the USB cable extenders.

Note: Angling the USB connectors slightly can avoid the need to remove the front faceplate when inserting USB cables.

The Netgate 4100 Rack Mount is ready to install into the rack.

Fig. 13: Do Not Put Tension On The Cable. The Cable Should Have Enough Length to be Removed Without Excessive Tension.

Fig. 14: Cut the Excess Cable Ties
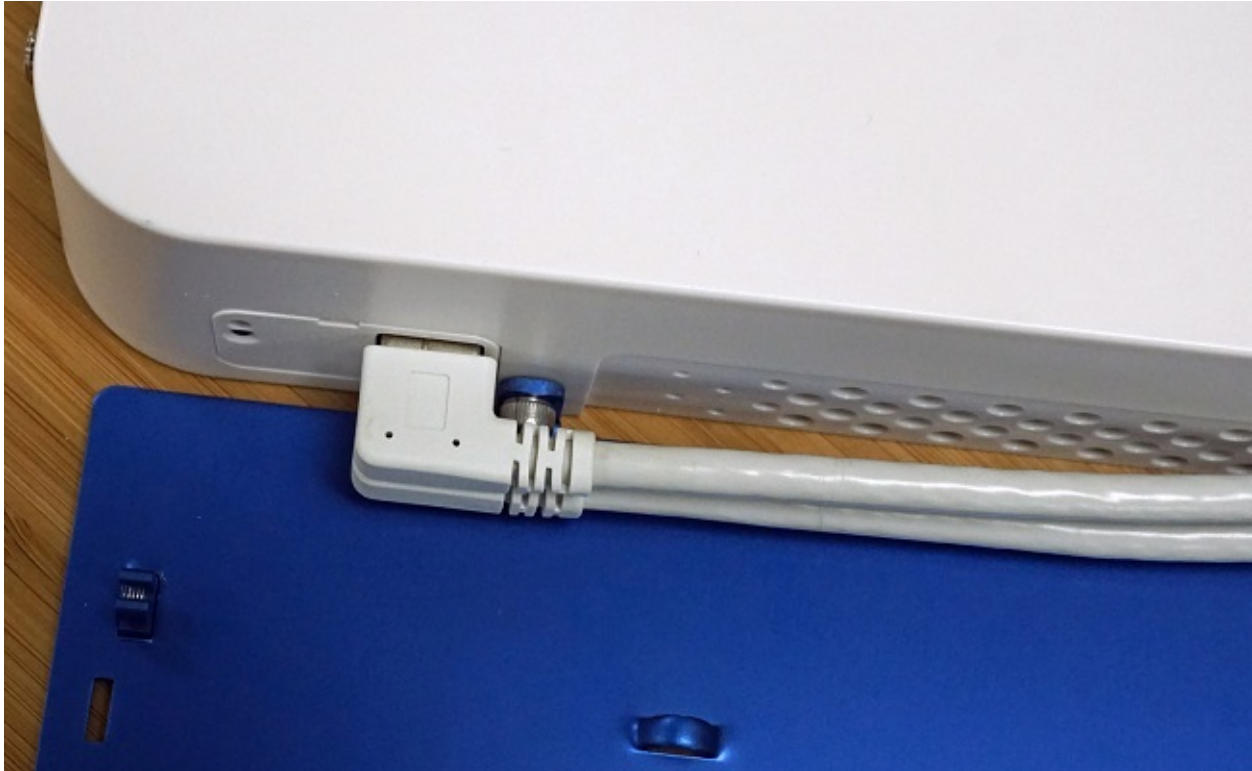
Fig. 15: Plug in the USB Cable Extenders

2.2 Netgate 4100 Wall Mount

The Netgate 4100 has an optional Wall Mount Kit available. This page provides an overview for attaching the system to the wall.

The Netgate 4100 can be mounted vertically or horizontally. If mounted horizontally, the ports and cables should face up to reduce the pull from the weight of the cables on the ports.

The Netgate 4100 Wall Mount Kit contains all the components necessary to mount the 4100.

The Netgate 4100 Wall Mount can be used in an *inboard* fashion, or an *outboard* fashion.

2.2.1 Inboard Wall Mount Instructions

Click on the button below to download the Wall Mount Template.

Note: The wall mount template is identical for the Netgate 4100, the Netgate 6100, and the Netgate 8200

Print the template out at **100% Scale** for it to be accurate.

Fig. 16: The Netgate 4100 Mounted Vertically

Fig. 17: The Netgate 4100 Wall Mount Kit

Fig. 18: The Netgate 4100 *Inboard* Wall Mount Orientation

Fig. 19: The Netgate 4100 *Outboard* Wall Mount Orientation
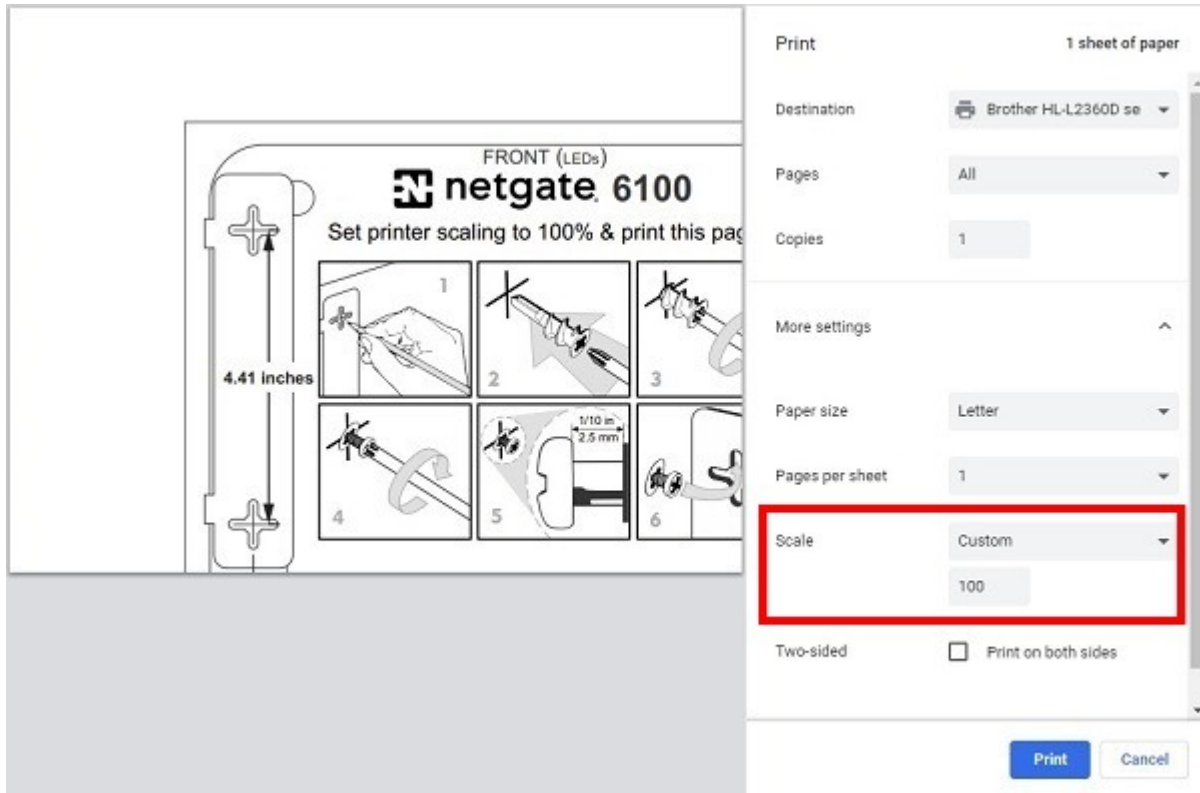
Note: The 100% Scale setting varies by printer manufacturer and model.

Follow the pictured instructions on the PDF to complete the wall mount installation.

2.2.2 Outboard Wall Mount Instructions

Click on the button below to download the Wall Mount Template.

Note: The wall mount template is identical for the Netgate 4100, the Netgate 6100, and the Netgate 8200.

There are two options to use the template:

1. Print out the first page at **100% Scale** on **8.5" x 17"** paper for it to be accurate.

2. Print pages 2 and 3 at **100% scale** on **8.5" x 11"** paper.

   Each page has a dotted line. Cut along the lines and verify the dimensions before using it.

Note: The mounting brackets themselves can also be used to make the wall markings.

Fig. 20: Using the Netgate 6100 Wall Mount Bracket to Mark the Screw Locations

2.2.3 Mounting the Power Supply

The mounting bracket for the power supply uses two zip-ties to hold the power supply to the mounting bracket. There is no PDF for the Power Supply Bracket. Use the holes directly to mark the wall for mounting.
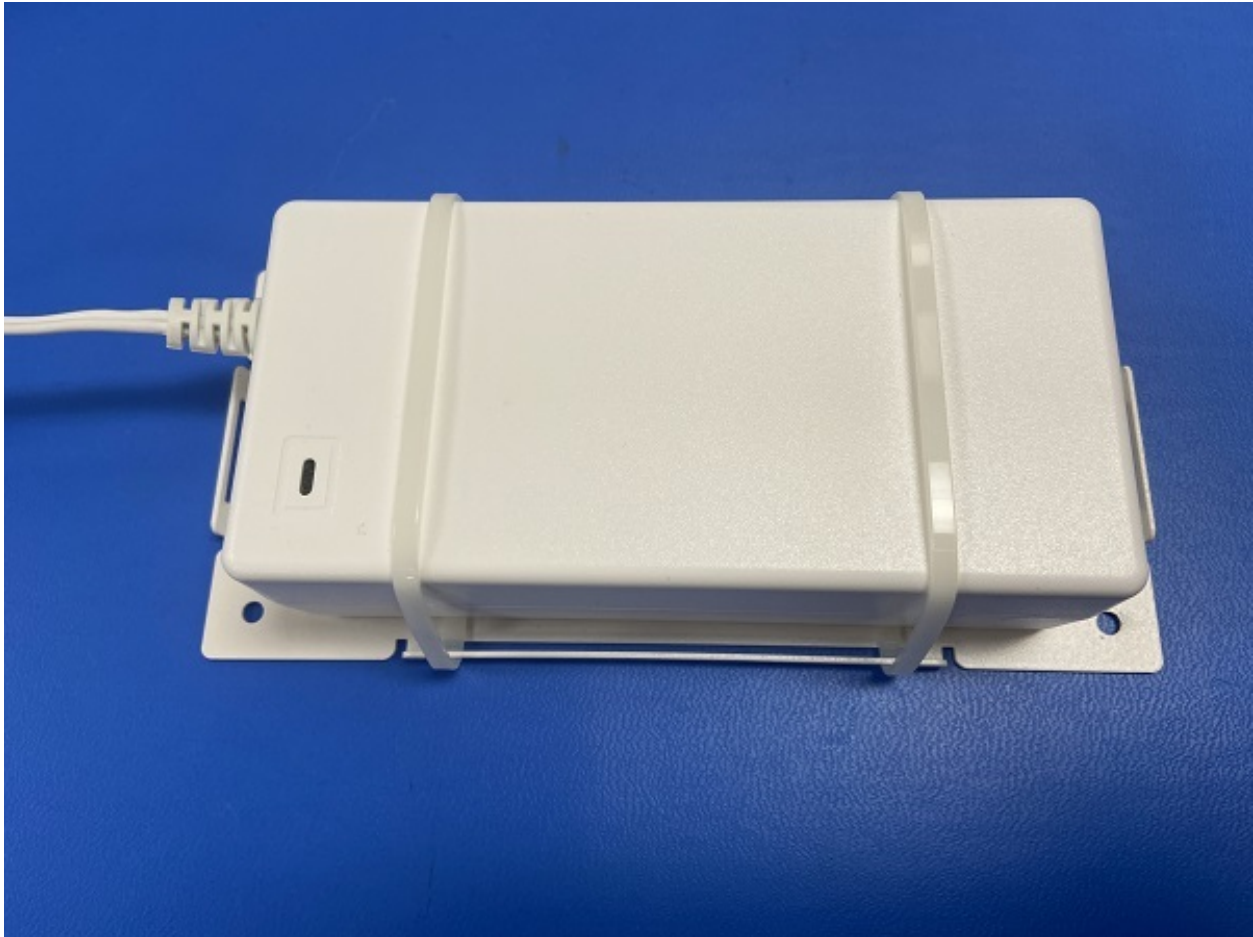
2.3 Connecting to the USB Console

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.

2.3.1 USB Serial Console Device

This device uses a **Silicon Labs CP210x USB-to-UART Bridge** which provides access to the console. This device is exposed via the **USB Micro-B (5-pin)** port on the appliance.

Install the Driver

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, connect to the console port using the cable that has a **USB Micro-B (5-pin)** connector on one end and a **USB Type A** plug on the other end.

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 hardware, the USB serial console port may not be detected by the client operating system until the device is plugged into a power source.

If the client OS does not detect the USB serial console port, connect the power cord to the device to allow it to start booting.

If the USB serial console port appears without power applied to the device, then the best practice is to wait until the terminal is open and connected to the serial console before powering on the device. That way 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.
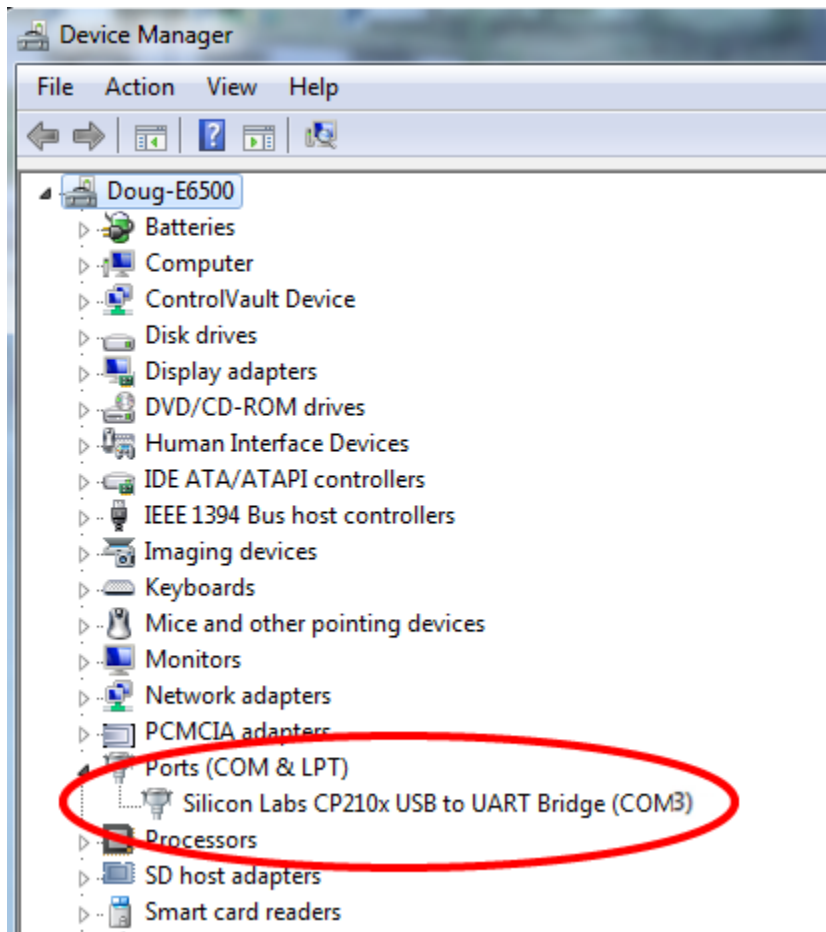
macOS

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.

2.3.2 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 on 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 on 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 on 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. 21: An example of using PuTTY on Windows

PuTTY on 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. 22: An example of using PuTTY on 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
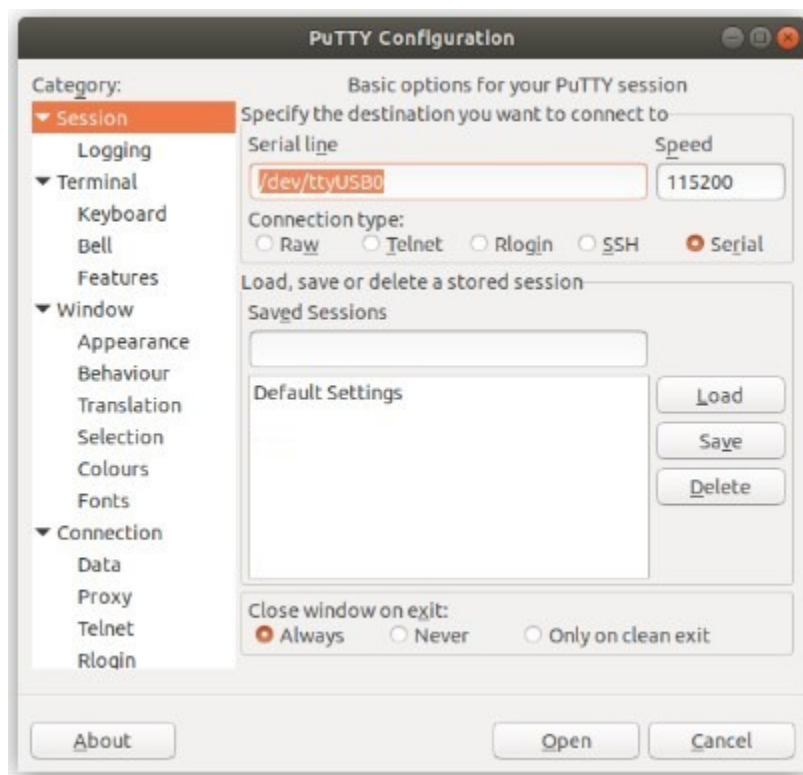
Beyond the required settings there are additional options in terminal programs which will help input behavior and output rendering to ensure the best experience. These settings vary location and client, and may not be available in all clients or terminals.

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 monospaced Unicode font such as DejaVu Sans Mono, Liberation Mono, Monaco, Consolas, Fira Code, or similar.

This setting may be under Terminal Appearance, Window Appearance, Text, or similar areas.

2.3.3 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 re-display 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.

2.3.4 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 installation 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**
>>> `80x24`
>
> **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 installation 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.

2.4 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.

2.4.1 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 on 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 on 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 on 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 on 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.
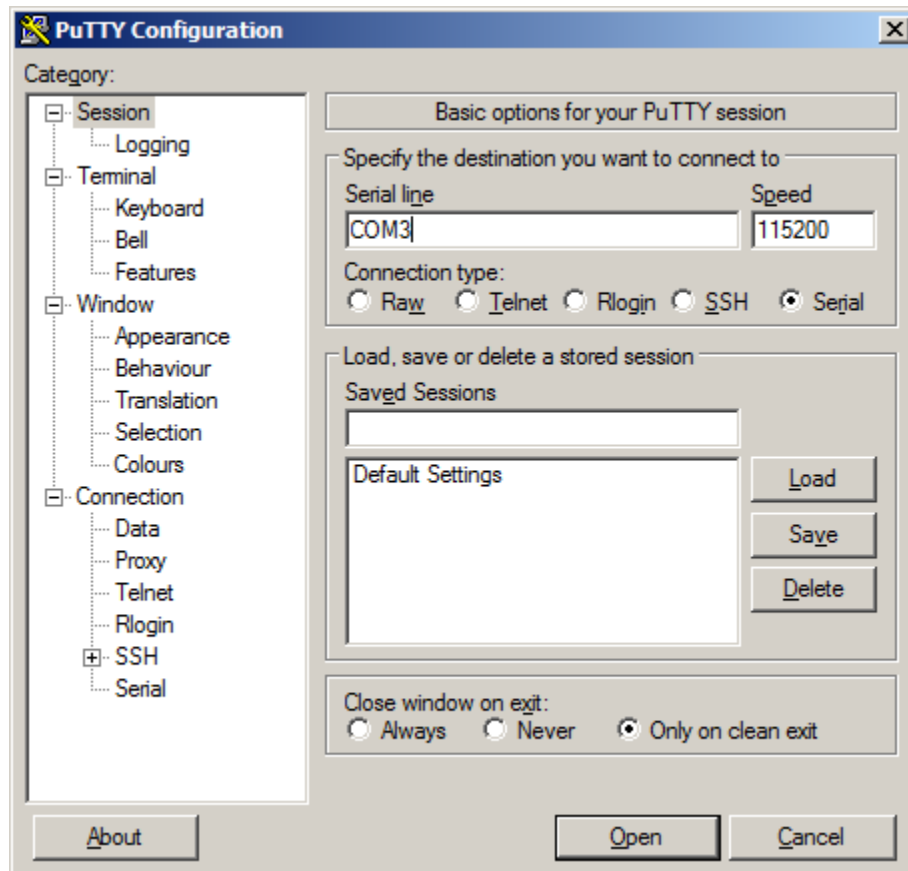
Fig. 23: An example of using PuTTY on Windows

Fig. 24: An example of using PuTTY on 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 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 monospaced Unicode font such as DejaVu Sans Mono, Liberation Mono, Monaco, Consolas, Fira Code, or similar.

This setting may be under Terminal Appearance, Window Appearance, Text, or similar areas.

2.4.2 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 re-display 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.

2.4.3 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 installation 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
`80x24`

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 installation 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.

2.5 Reinstalling pfSense Plus Software

This guide uses the Netgate Installer to install pfSense® Plus software on a **Netgate 4100** device.

Note: pfSense® Plus is preinstalled on Netgate appliances. It is optimally tuned for Netgate hardware and contains features that cannot be found elsewhere, such as ZFS Boot Environments, OpenVPN DCO, Built-in IPFIX Export, and the AWS VPC Wizard.

2.5.1 Download Installation Media

The Netgate Installer can be downloaded from the Netgate Store using a Netgate Store Account.

See also:

For a more detailed walkthrough of the download process, see Download Installation Media in the pfSense Software Documentation.

The image to download for this device is:

`netgate-installer-amd64.img.gz`

2.5.2 Prepare Installation Media

Next, write the installation 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.

2.5.3 Connect to the Console

The installation process is interactive and utilizes the console. Follow the directions under *Connect to the console* to configure and use the console.

2.5.4 Boot the Installation Media

Insert the memstick into an open USB port and boot the device.

Note: If the device does not automatically boot from USB, restart the device again and press `F2` when prompted to start the boot selection menu, then select the USB drive.

2.5.5 Determine Target Drive

During the installation process the installer will prompt to select a target drive. The installer will then write pfSense®
Plus to the chosen drive. In most cases a device will have only one potential target drive.

- On devices with only MMC storage, the only choice is `mmcsd0`.
- On devices with only NVMe storage, the only choice is `nda0`.
- On devices with multiple drives take care to choose the correct intended target.

    Tip: If the device contains NVMe storage (`nda0`), such as a MAX variant, that is the optimal choice.

- USB storage devices appear as `daX` where `X` is a device number, such as `da1`. The device number may shift depending on the order in which the OS probes USB devices or the order in which they are inserted while the OS is running.

    Note: The installation media is also a USB drive, but the installer does not offer its own disk as a target drive.

2.5.6 Install pfSense Plus Software

The installer will automatically launch and present several options. On Netgate appliances, choosing `Enter` for the default options will complete the installation process in most cases.

Tip: There are options on the Welcome screen of the installer which can recover configuration data from a previous installation or from a USB drive.

See also:

For a complete walkthrough of the installation process, see Installation Walkthrough.

When the installation is complete, remove the USB drive from the USB port.

Important: If the USB drive remains attached, the device 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.

2.6 Configuring an OPT interface as an additional WAN

Note: The default configuration has all ports assigned as WANs and LANs to match the labels on the back of the device. These are only pre-defined labels; any port can be renamed and configured for any purpose.

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

See also:

Multi-WAN documentation

Configuring an additional WAN

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

2.6.1 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.

2.6.2 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 created first (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** and the customized name **WAN2**.

The newly assigned interface will have its own entry under the **Interfaces** menu and elsewhere in the GUI.

2.6.3 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 on WAN 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

2.6.4 Outbound NAT

For clients on local interfaces to reach 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 and follow the section below which matches the mode.

Automatic or Hybrid Outbound NAT

If the mode is set to **Automatic** or **Hybrid**, then this may not need further configuration.

Ensure there are rules for the new WAN listed as an **Interface** in the **Automatic Rules** at the bottom of the page. If so, skip ahead to the next section to configure Firewall Rules.

Manual Outbound NAT

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
  Either choose *LAN Subnets*, which will automatically reference any networks on the LAN interface, or choose *Network or Alias* and manually fill in the LAN subnet, e.g. `192.168.1.0/24`.

  If there are multiple local networks, create rules for each or use other methods such as aliases or CIDR summarization to cover them all.

  Destination
  Any

  Translation Address
  WAN2 Address (or the custom name of the new WAN interface)

  Description
  Text describing the rule, e.g. `LAN outbound on WAN2`

- Click **Save**

- Click **Apply Changes**

Repeat as needed for additional local networks.

2.6.5 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.

2.6.6 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**, Gateway for 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**, Gateway for 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
        `Load Balance Connections on WAN and WAN2`

Note: Rules using this group enable connection-based load balancing, not per-packet load balancing.

Rules using this group will also have failover style behavior as WANs which are down are removed from load balancing.

- 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.

2.6.7 DNS

DNS is critical for Internet access, and it is 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 in the **DNS Server Settings** section, ideally two or more. Click

    ╋ **Add DNS Server** to create additional rows.

    Each entry should be configured as follows:

    Address
    The IP address of a DNS server.

    Each server address **must be unique**, the same server **cannot** be listed more than once.

    DNS Hostname
    Leave this field blank unless the server will be contacted using DNS over TLS through the DNS Resolver. In this case, enter the FQDN of the DNS server, so its name can be validated against its TLS certificate.

    Gateway
    Select a gateway for each DNS server, corresponding to the WAN 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.

    Note: If the gateway drop-down does not appear next to each DNS server, then the firewall does not have more than one gateway configured for any address family. Double-check the gateway settings for all WAN interfaces.

- 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.

2.6.8 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 subnets*

  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**

2.6.9 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 is 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.

2.6.10 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 from WAN2 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.

2.6.11 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 ISP Customer Premise Equipment (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.

2.7 Configuring an OPT interface as an additional LAN

Note: The default configuration has all ports assigned as WANs and LANs to match the labels on the back of the device. These are only pre-defined labels; any port can be renamed and configured for any purpose.

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

2.7.1 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`.

2.7.2 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 created first (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.

2.7.3 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 **IPv4 Address** and CIDR mask for the new LAN

  For this example, 192.168.2.1/24.

- **Do not** add or choose an **IPv4 Upstream 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

2.7.4 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.

This configuration varies slightly depending on the DHCP server and version.

See also:

DHCPv4 Configuration

- Navigate to **Services > DHCP Server**, **OPTx** tab (or the custom name)

- Check **Enable**

- Configure the **Address Pool 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 of the settings can be left at defaults

- Click **Save**

2.7.5 Outbound NAT

For clients on this interface to reach 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 and follow the section below which matches the mode.

Automatic or Hybrid Outbound NAT

If the mode is set to **Automatic** or **Hybrid**, then this likely does 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.

Manual Outbound NAT

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
  Either choose *OPTx Subnets*, which will automatically reference the new interface, or choose *Network or Alias* and manually fill in the new subnet, e.g. `192.168.2.0/24`.

  Destination
  Any

  Translation Address
  WAN Address (or the customized name matching the WAN/egress interface)

  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.

2.7.6 Firewall Rules

By default, there are no firewall rules on the new interface, so the firewall will block all traffic. This is not ideal for a LAN as generally speaking, the clients on this LAN 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 subnets* (or the custom name)
>
> **Destination**
>> *Any*
>
> **Description**
>> Text describing the rule, e.g. `Default allow all from OPTx`

- Click **Save**

- Click **Apply Changes**

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 with additional 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:** A full set of reject rules as described in this example is the best practice. Do not rely on shortcuts such as using policy routing to isolate clients.

Create a Private Networks Alias

Create an alias using all RFC 1918 networks (listed in the example below) or at least an alias containing the local/private networks on this firewall, such as VPNs. Using all RFC 1918 networks is a safer practice.

- Navigate to **Firewall > Aliases**

- Click **Add**

- Configure the alias 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**

Add Firewall Rules

With the alias in place, the next task is to create firewall rules for the interface.

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

Allow DNS

Add rule to allow DNS requests from local clients to the firewall itself 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 subnets* (or the custom name)

Destination
This Firewall (self)

If clients are configured to query DNS servers other than this firewall, create rules using those as the destination instead.

Destination Port Range
Select the *DNS (53)* entry or choose *Other* and manually enter 53

To allow DNS over TLS, create a separate rule using the *DNS over TLS* entry or manually enter port 853.

Description
Text describing the rule, e.g. `Allow clients to resolve DNS through the firewall`

- Click **Save**

Allow ICMP to the Firewall

Add a rule to allow ICMP traffic from local devices to the 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

  Tip: While ICMP is useful, some network administrators prefer to limit the allowed ICMP types to *Echo Request* only. This allows devices to use ICMP ping for diagnostic purposes, but no other types of ICMP traffic.

  Source
  OPTx subnets (or the custom name)

  Destination
  This Firewall (self)

  Description
  `Allow client ICMP to the firewall`

- Click **Save**

Reject Other Firewall-bound Traffic

Add rule to reject any other traffic to the firewall to ensure users on this interface cannot connect to management services such as the GUI, SSH, and so on.

- Click ![Add] 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
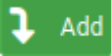   > `Reject all other traffic to the firewall`

- Click **Save**

Reject Private Traffic

Add rule to reject traffic from this network to all other private networks.

- Click ![Add] 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
   > *Address or Alias*, `PrivateNets` (the alias created earlier)

   Description
   > `Reject all other traffic to private networks`

- Click **Save**

Allow Other Traffic

Add rule to allow traffic from this interface network to any other destination, which enables clients on this interface to reach the Internet and/or other remote public networks.

- Click ⬇ Add 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 subnets* (or the custom name)

  Destination
  > *Any*

  Description
  > ``Default allow all from OPTx``

- Click **Save**

Apply Changes

With the rules all in place, click **Apply Changes** to finish and activate the new rules.

The rules should look similar to the following figure:

Fig. 25: Example firewall rules for isolated LAN type segment

---

Tip: Rule separators are useful for documenting a ruleset in place.

Similar to the isolated network scenario, it is also possible to be much more strict with rules to only allow specific outbound ports. When creating this type of configuration,

2.7.7 Other Services

In most cases the above configuration is sufficient and clients on the new LAN can now obtain an address and reach 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

2.8 Factory Reset Procedure

This procedure performs a factory reset using the hardware reset button on the Netgate 4100. This button is located on the left side of the unit when facing the front (See *Input and Output Ports* for reference photos).

See also:

- Factory Reset from GUI or Console

1. Shut down or remove power from the device.

2. Power on the device.

3. Wait for the **circle** LED to change from orange to blue.

4. Press and hold the reset button (top) for **5 seconds**.

Note: This is the top (recessed) button and may require a pen, paperclip, or similar tool to press.

This "short press" of the button initiates the reset procedure.

After the system mounts the drive, it recognizes that the button had a short press, and then it prompts to confirm the reset by turning all the LEDs solid red.

5. Wait for the LEDs all change to solid red.

6. Hold the reset button until all three LEDs start flashing red

This will take approximately **13 seconds**

The system then resets the configuration and reboots.

7. 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 light slowly flashing 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.

2.9 M.2 NVMe SSD Installation

The Netgate® 4100 has built-in onboard eMMC storage. Optionally, a PCIe-based M.2 NVMe drive can be installed as an upgrade or to bypass the onboard eMMC flash memory.

Note: The Netgate 4100 has a MAX variant which includes an M.2 NVMe drive. MAX variants ship with the operating system installed on the NVMe drive and with the eMMC empty.

M.2 NVMe SSD Installation Outline

- *Warnings and Precautions*
- *Required Tools and Hardware*
- *Installation Procedure*

2.9.1 Warnings and Precautions

Danger: **Anti-static protection must be used throughout this procedure**.

Warning: If pfSense® Plus software is installed on the eMMC storage, it **must be wiped** from the onboard eMMC storage before reinstalling pfSense Plus software on the M.2 NVMe SSD. This is covered *later within the installation procedure* in this document.

For more details on why this is necessary and how to wipe the disk, see https://docs.netgate.com/pfsense/en/latest/troubleshooting/multiple-disks.html

Warning: The Netgate 4100 is only compatible with PCIe-based M.2 NVMe storage devices. It is **not compatible with** M.2 SATA devices.

The Netgate 4100 has one socket compatible with a PCIe-based M.2 NVMe drive. This is a **B-key** socket which accepts M.2 **B+M-key** or **B-key** PCIe NVMe SSDs **only**.

Danger: Take all appropriate precautions and exercise care when handling the exposed system board and M.2 card. There are many delicate components which can be damaged during this process. **Damage caused via physical contact and electrostatic discharge while performing this installation is not covered by the warranty**.

2.9.2 Required Tools and Hardware

Installing an M.2 NVMe SSD in the Netgate 4100 requires the following tools and hardware:

- #1 Phillips screwdriver
- T10 Torx driver

- T6 Torx driver

- Anti-static grounding strap and anti-static mat for handling bare M.2 card and 4100 system

- 1 x PCIe-based M.2 NVMe SSD, 2242 or 2280 size, **B+M-key** or **B-key** card

2.9.3 Installation Procedure

The installation procedure has many steps which are broken down into related groups in the remainder of this document. Follow all steps in the procedure carefully.

Take a Backup

If the system contains an existing configuration which should be carried over to the new SSD, then the first step is to take a backup of that configuration.

If the existing configuration is not necessary, this section may be skipped.

There are numerous backup options covered in the pfSense software documentation section on Backup and Restore.

For the purposes of reinstalling and restoring, the easiest method is to take a local backup.

Download the Installer

Before proceeding further, download a copy of the Netgate Installer amd64 memstick image using a Netgate Store Account and write the installer to a USB memstick. For details, see *Reinstalling pfSense Plus Software*.

Wipe the eMMC

To ensure the old installation of pfSense software on the eMMC does not interfere with the new installation of pfSense software on the SSD, the metadata on the eMMC must be wiped.

> **Warning:** Do not skip this procedure. Failing to wipe the eMMC may result in installation failures, upgrade failures, or other unpredictable behavior from having two conflicting installations present.

1. *Connect to the serial console*

2. Boot the Netgate Installer

3. Choose the option to start a **Rescue Shell** when prompted

4. Follow the rest of the procedure for wiping the disks in the pfSense software documentation at https://docs. netgate.com/pfsense/en/latest/troubleshooting/multiple-disks.html

---

Note: The eMMC storage device will appear as `mmcsd0`. When following the procedure to wipe the disks, use that device.

After wiping the eMMC, run the command `shutdown -p now` from the rescue shell to cleanly shut down and power off the device.

Power Off and Disconnect

Installing the SSD requires removing the top of the case to expose the internal components. Before opening the case, the Netgate 4100 must be **completely** disconnected from everything. This includes power, network cables, USB cables, serial console cables, and any other cable or devices connected to the Netgate 4100.

> **Danger: Reminder:**
> - Anti-static protection must be used throughout this procedure.
> - Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Unplug the power cable

> **Danger:** Wait at least **60 seconds** after unplugging power to proceed. This ensures that all phantom power has dissipated.

2. Unplug all network cables, USB cables and devices, serial console connections, etc.
3. Dismount the Netgate 4100 device
4. Move the Netgate 4100 to a safe work location such as an anti-static mat

Removing the Lid

The next portion of the procedure involves opening the device and removing the lid.

> **Danger: Reminder:**
> - Anti-static protection must be used throughout this procedure.
> - Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Turn the device over carefully and protect the surface to avoid damaging the lid of the device

> **Tip:** An anti-static mat or similar non-marring work surface is ideal for this role.

2. Locate and remove the six (6) T10 Torx and two (2) T6 Torx screws holding the chassis together using appropriately sized Torx drivers.
3. Gently remove the bottom panel.
4. Turn the device so the I/O panel ("rear" of the system) is visible.
5. Gently pull the edge of the plastic lid at the right corner of the device away from the base only far enough for the lid to clear the SIM card slots.
6. Separate the remainder of the lid from the chassis and system board.
7. Set the lid off to the side, keeping it upright to avoid damaging the top surface.
8. Turn the chassis upright so that the system board is visible.
9. Set the upright system flat on its base.
10. Turn the device so the I/O panel ("rear" of the system) is visible.
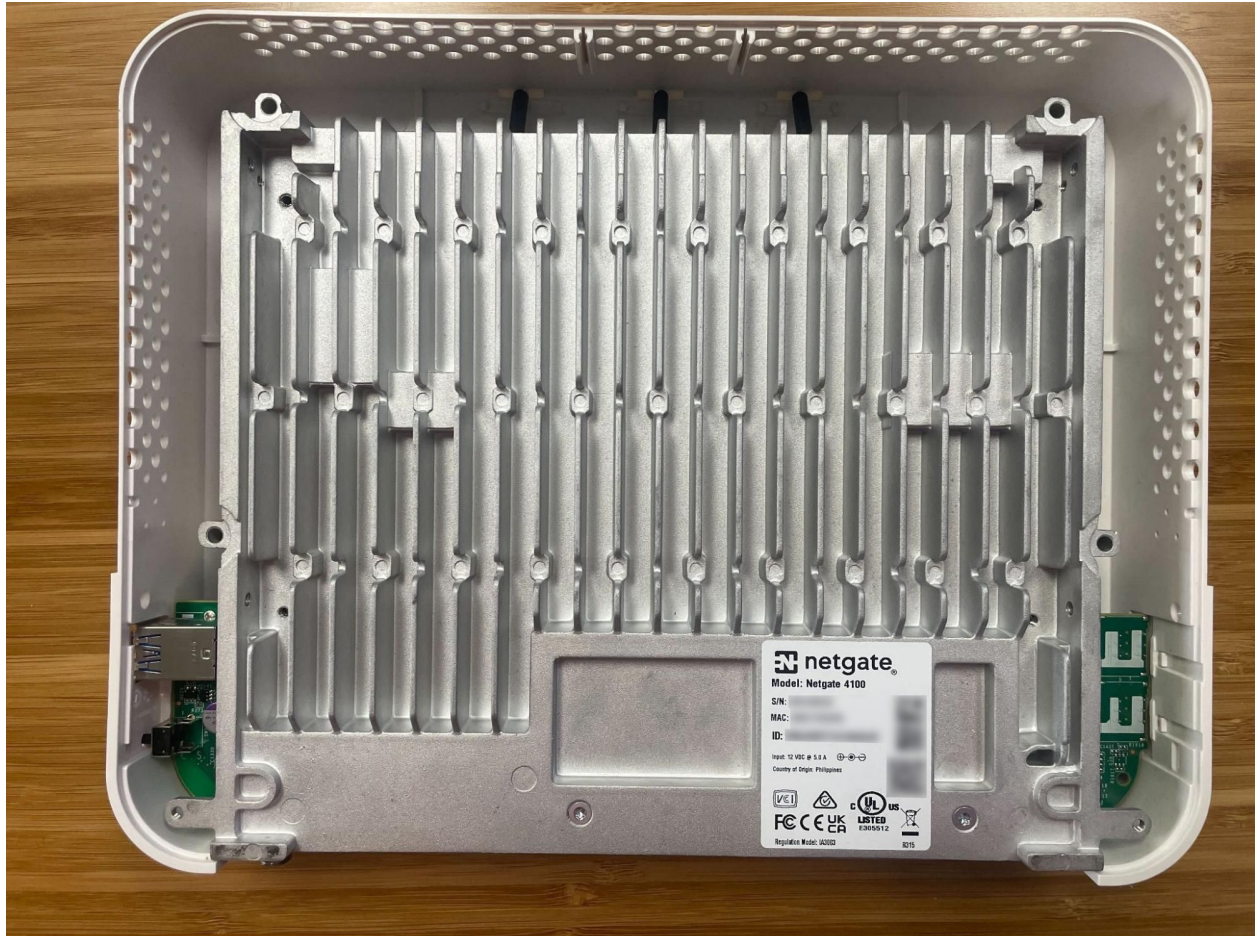
Fig. 26: Netgate 4100 case screw locations

Fig. 27: Netgate 4100 with bottom panel removed

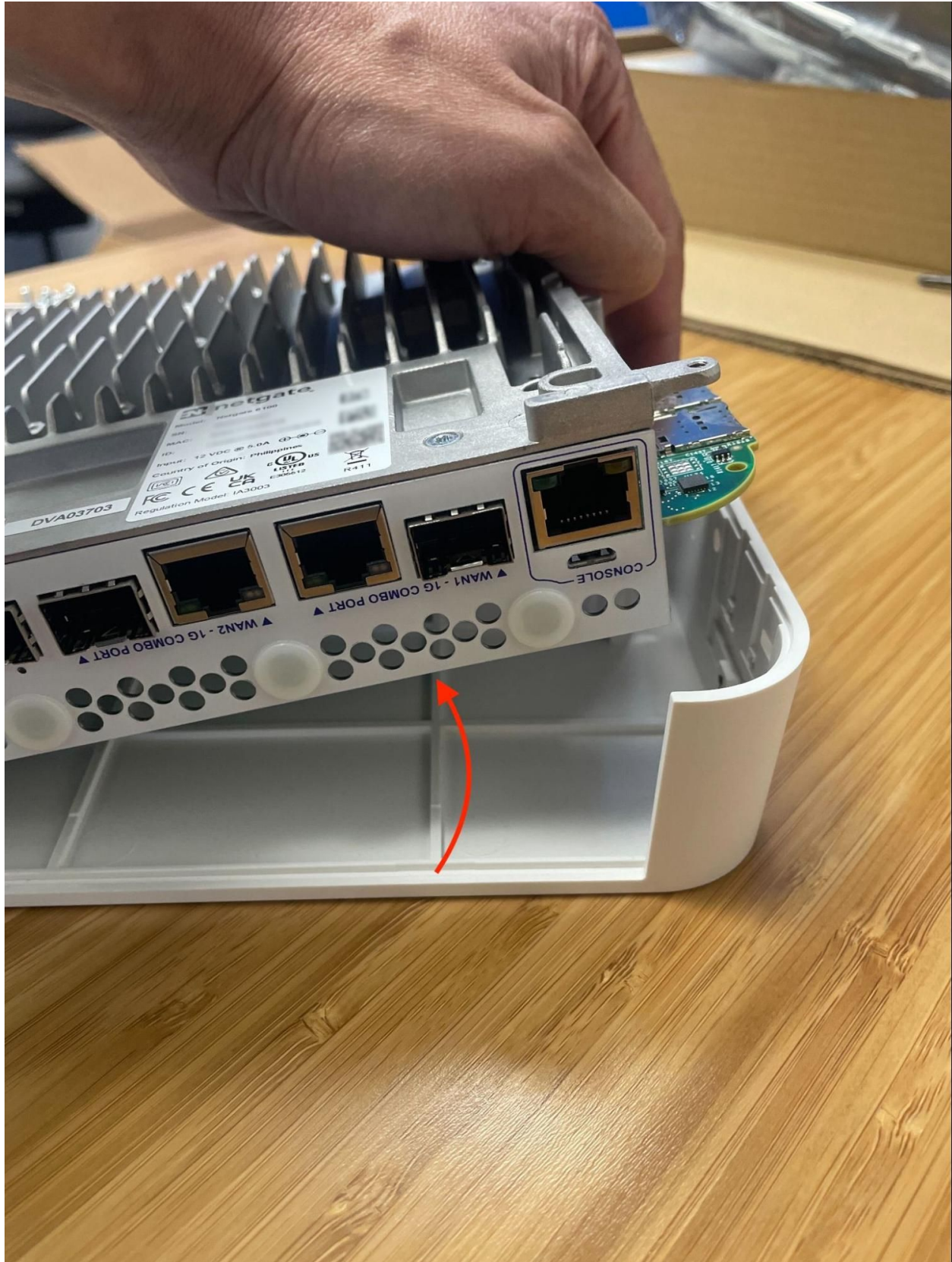Fig. 28: Removing the lid while clearing the SIM card slots

Fig. 29: Removing the Netgate 4100 chassis from the lid

Install the SSD

Now that the lid is removed, it is time to install the SSD.

Danger: Reminder:

- Anti-static protection must be used throughout this procedure.

- Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

---

1. Locate the M.2 socket in which the M.2 NVMe SSD will be installed.

   With the device in the proper orientation, it is approximately halfway up the left side of the board.

   Note: As mentioned earlier in this document, the Netgate 4100 is compatible with M.2 **B+M-key** or **B-key** PCIe NVMe SSDs **only**.
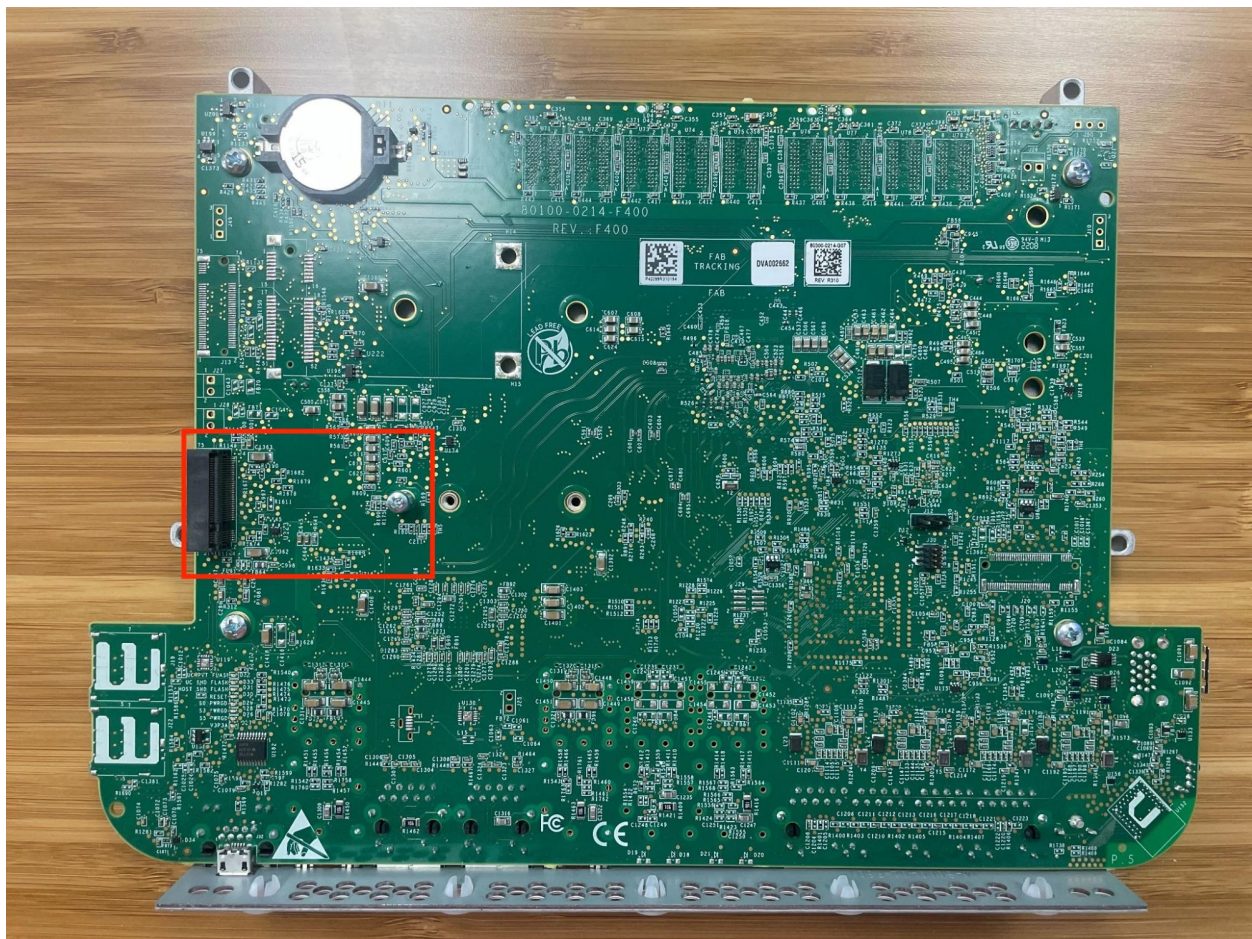

Fig. 30: Netgate 4100 top-down internal view with the M.2 socket highlighted

2. Remove the retention screw from the standoff using the #1 Phillips head screwdriver.

3. Move the standoff to the appropriate hole for the SSD length (2242 or 2280) if it is not already in the correct location.

4. Insert the M.2 card into the socket at an approximate 30° angle.

> **Warning:** M.2 cards are keyed. **Do not** force an M.2 card into a slot with mismatched keying.
>
> Refer to M.2 Edge Connector Keying for a depiction of the different M.2 key types.

Fig. 31: Inserting the SSD into the M.2 socket at an angle

5. Gently push down the M.2 NVMe card until it reaches the standoff.

6. Insert the retention screw into the standoff and tighten using the #1 Phillips head screwdriver.

Replacing and Fastening the Lid

With the M.2 NVMe SSD in place, the next step is to replace the lid and all the fasteners.

> **Danger: Reminder:**
> - Anti-static protection must be used throughout this procedure.
> - Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

1. Align the USB ports on the left side with the matching holes in the lid.

2. Align the internal groove in the lid with the edges of the I/O panel.

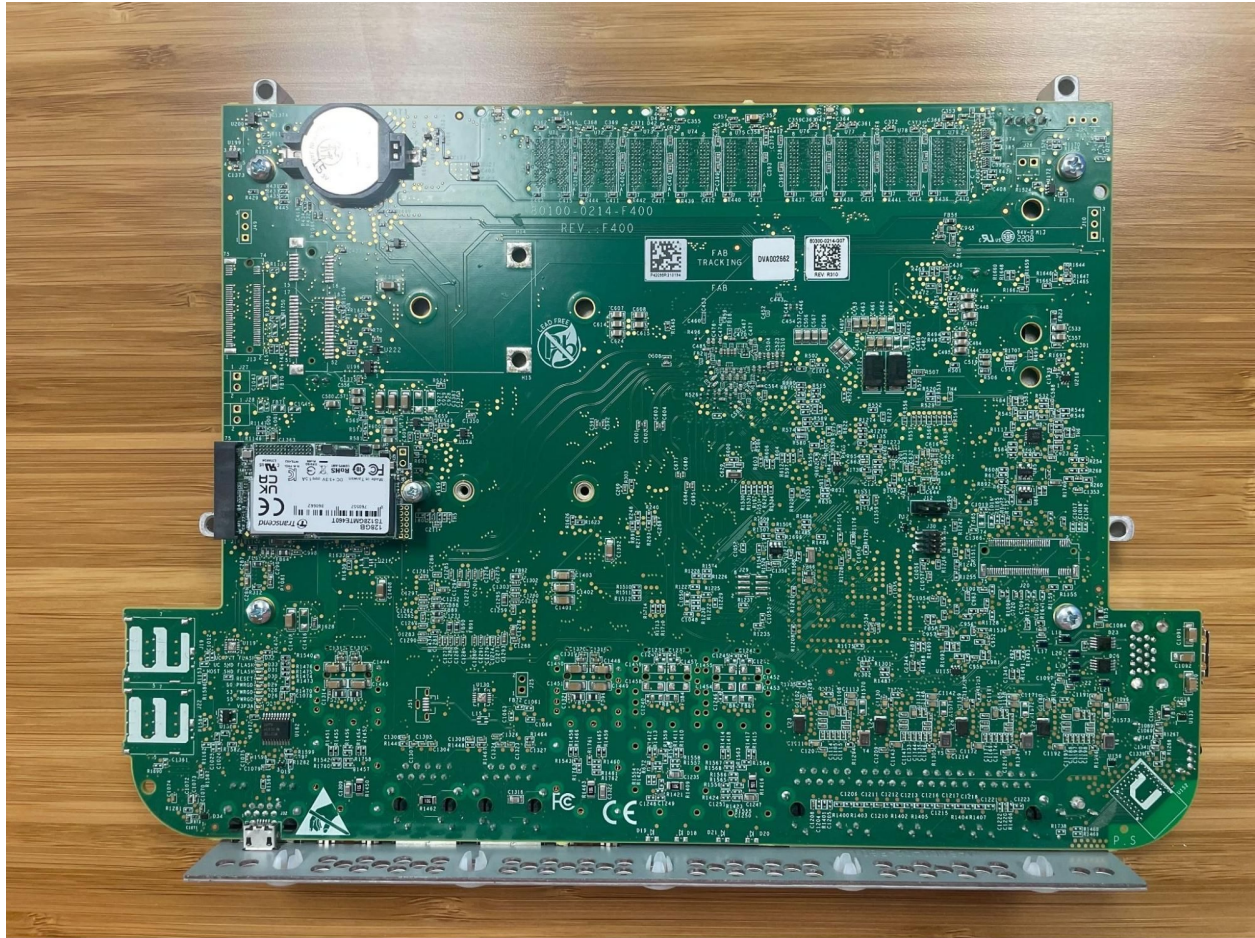3. Lower the left edge of the lid onto the chassis.

Fig. 32: 2242 length M.2 NVMe SSD installed and secured with retention screw

Fig. 33: Aligning the left edge of the lid with the USB ports and I/O panel

4. Continue lowering the chassis until the lid until the right side is at the edge of the lid.

5. Gently pry the right side of the lid away from the chassis enough to clear the SIM card slots while simultaneously lowering the chassis.

   The lid should click into place over the SIM card slots.

6. Check the rear corners of the lid to make sure the I/O panel is fully seated in the lid grooves.

7. Check the alignment of the plastic lid edges with the metal baseplate, SIM card slots, USB A opening, etc.

8. Replace the bottom panel.

9. Replace the six (6) T10 Torx and two (2) T6 Torx screws holding the chassis together using appropriately sized Torx drivers.

Reconnect

The device is now ready to be put back into its former location.

1. Move the device back to its original location.

2. Re-mount the Netgate 4100 device

3. Plug in all network cables, USB cables and devices, serial console connections, etc.

4. Insert the USB memstick containing the installation media

5. Plug in the power cable

6. Reconnect to the serial console

Reinstall pfSense Plus Software

With the device back together and ready to proceed, the next step is to reinstall pfSense Plus software to the SSD. This procedure is covered in detail in *Reinstalling pfSense Plus Software*.

Note: If prompted to select a drive during the installation, choose the NVMe drive which will be `nda0`. The installer will typically select this drive automatically, but double check to be certain it is correct.

The eMMC drive (`mmcsd0`) should remain **deselected** so it will not be used by the installer.

If there is no backup to restore, then no further steps are necessary. Login to the firewall and configure it as normal (*Initial Configuration*).

Restore the Configuration

The final step is to restore the configuration. If a configuration was *backed up earlier in this procedure*, now is the time to restore it using the GUI or one of the other methods mentioned in the pfSense software documentation section on Backup and Restore.

Fig. 34: Replacing the lid while clearing the SIM card slots

Fig. 35: Netgate 4100 case screw locations

REFERENCES

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 assistance 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 Netgate appliances and for other helpful resources, make sure to browse the Netgate Resource Library.

https://www.netgate.com/resources

3.1.3 Professional Services

Netgate TAC 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

Customers who elected not to get a Netgate TAC plan, can seek assistance from the active and knowledgeable pfSense software community on the Netgate forum.

https://forum.netgate.com/

3.2 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.