



Security Gateway Manual

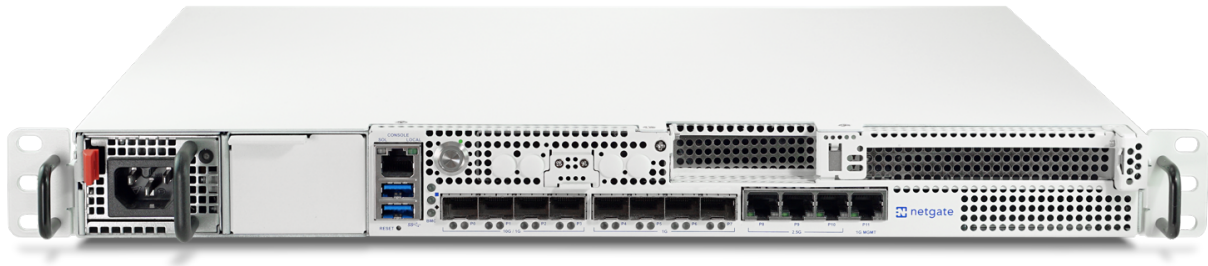
Netgate-8300

© Copyright 2024 Rubicon Communications LLC

Nov 08, 2024

CONTENTS

1	Out of the Box	2
2	How-To Guides	30
3	References	143



This Quick Start Guide covers the first time connection procedures for the [Netgate® 8300 Security Gateway](#) 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.

1.1.1 Remove Protective Wrap

The **Netgate 8300** ships with clear plastic overwrap on the **top and bottom** of the unit to protect the panels from scratches before installation. Remove this overwrap before continuing the setup process.

<p>Warning: The plastic overwrap must be removed from both the top and bottom of the unit before installing the device in a rack.</p>
--

1.1.2 Rack Installation

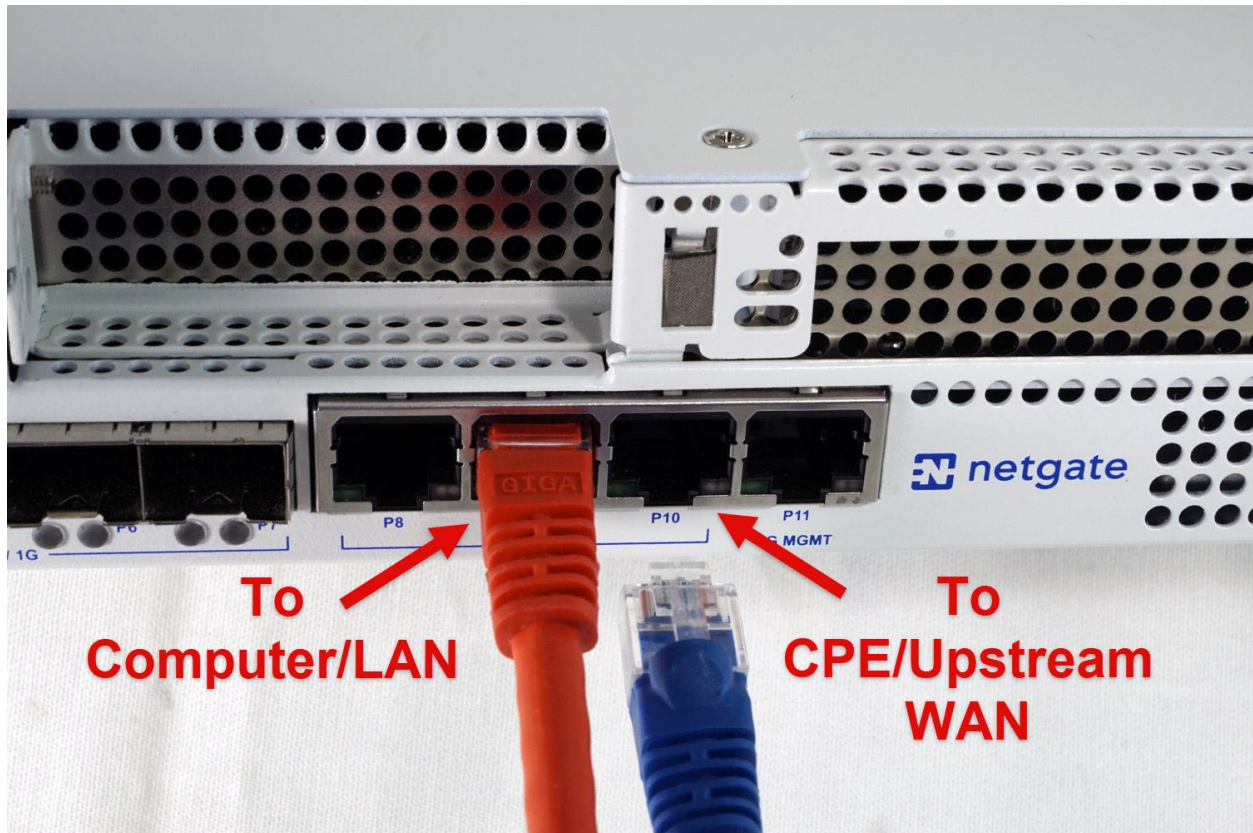
The **Netgate 8300** is intended to be rack mounted. The best practice is to mount the unit in a rack before connecting it to the network or power.

1.1.3 Connect Network Cables

Connect one end of an Ethernet cable to the P10 port (shown in the *Input and Output Ports* section) of the Netgate appliance. Insert the other end of the same cable into the upstream network connection. For example this might be an ISP Customer Premise Equipment (CPE) device, such as a cable or fiber router, or an external switch, such as one connecting to a datacenter WAN.

Note: 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 P9 port (shown in the *Input and Output Ports* section) of the Netgate appliance. Connect the other end to the computer or a downstream LAN switch.

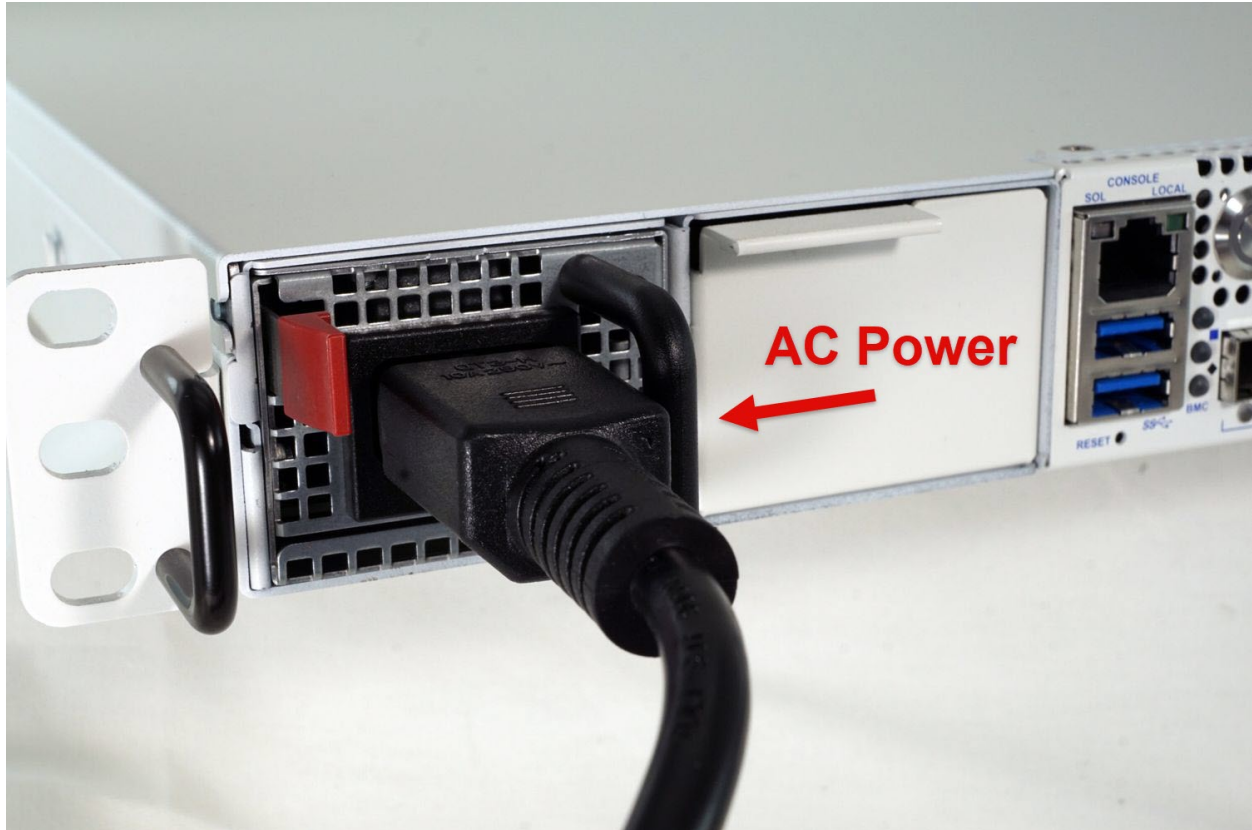


1.1.4 Connect Power

The **Netgate 8300** ships with one or two power supplies depending on the specific model or purchased add-ons. Connect power to all installed power supplies before powering on the unit.

Note: Though the device can function with only a single power supply connected, the best practice is to always connect power to both power supplies.

After connecting power, turn on the power switch located on the rear of the unit.



1.1.5 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 Console Port](#).

Warning: The default IP Address on the LAN subnet on the Netgate firewall is 192.168.1.1/24. The same subnet **cannot** be used on both WAN and LAN, so if the default IP address on the ISP-supplied modem is also 192.168.1.1/24, **disconnect 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.

Warning: This device includes an intrusion detection sensor which operates even when the device is without power.

Opening the case on this device triggers an intrusion alarm which is logged by the BMC and is visible in the IPMI sensors. **This alarm must be reset manually** as described in [Re-arm the Chassis Intrusion Switch](#).

When the intrusion alarm is active the fans run at a fixed speed of around 8500 RPM. Resetting the intrusion sensor alarm returns the fans to their profiled speed.

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 **P10** port on the Netgate 8300 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.

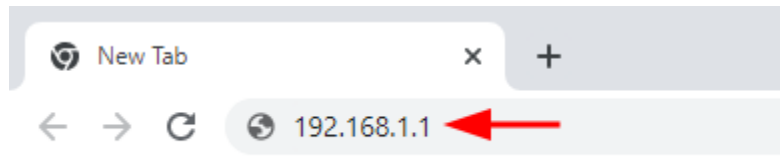


Fig. 1: Enter the default LAN IP address in the browser

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

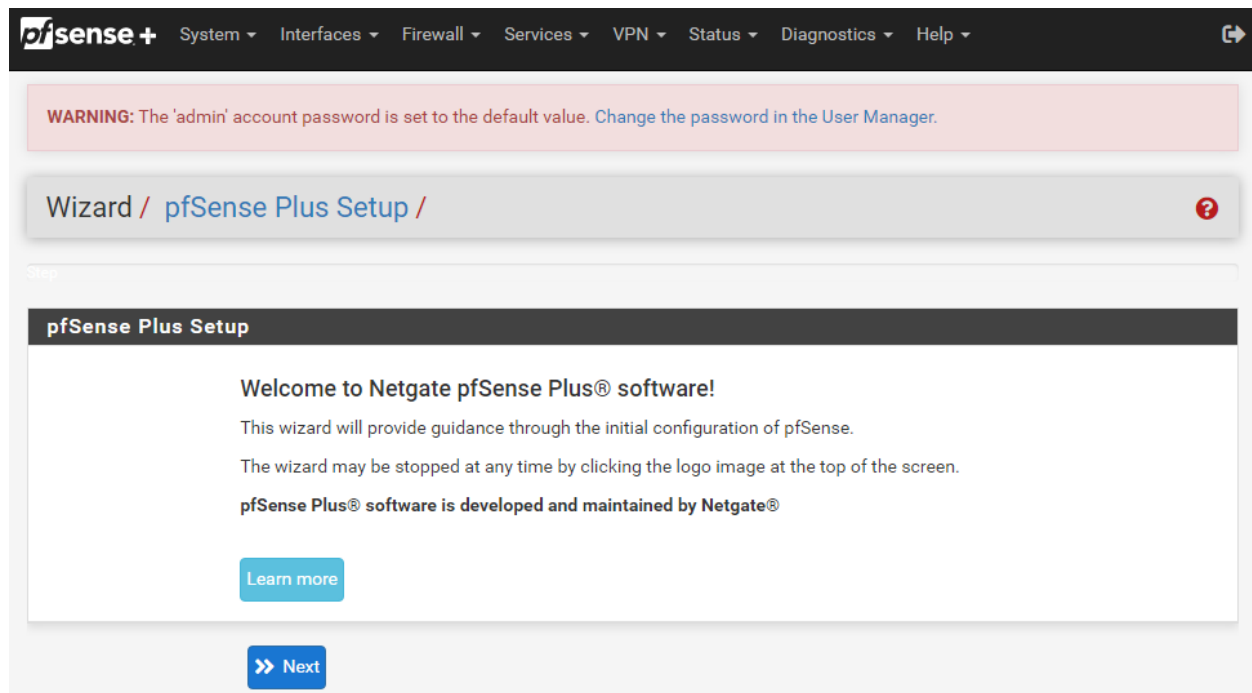


Fig. 3: Setup Wizard starting page

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.

Wizard / pfSense Plus Setup / General Information 

Step 2 of 9

General Information

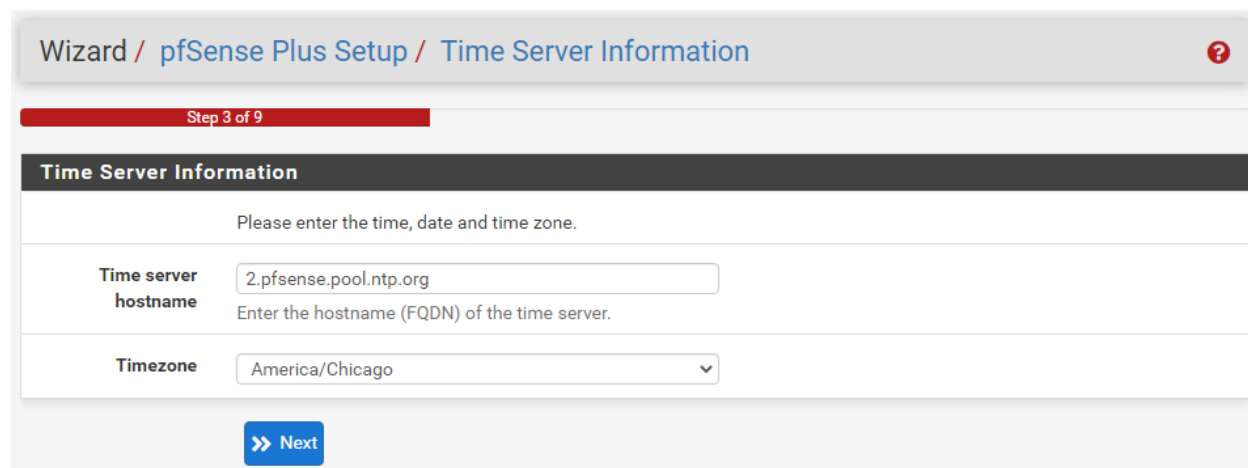
On this screen the general pfSense Plus parameters will be set.

Hostname	<input type="text" value="pfSense"/> EXAMPLE: myserver
Domain	<input type="text" value="home.arpa"/> EXAMPLE: mydomain.com
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
Primary DNS Server	<input type="text" value="8.8.8.8"/>
Secondary DNS Server	<input type="text" value="8.8.4.4"/>
Override DNS	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

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

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



Wizard / pfSense Plus Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

[Next](#)

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 **P10** port on the Netgate 8300 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.

Wizard / pfSense Plus Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

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

SelectedType

DHCP

General configuration

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

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 **P10** 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.

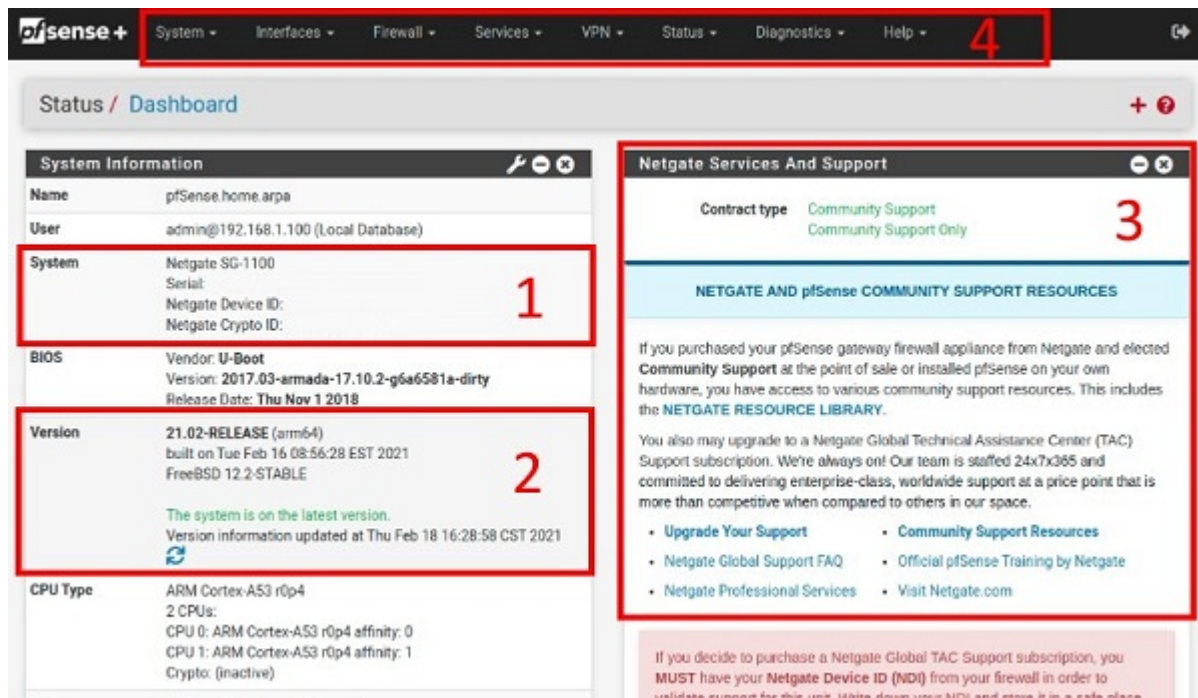


Fig. 8: The pfSense® Plus Dashboard

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**.

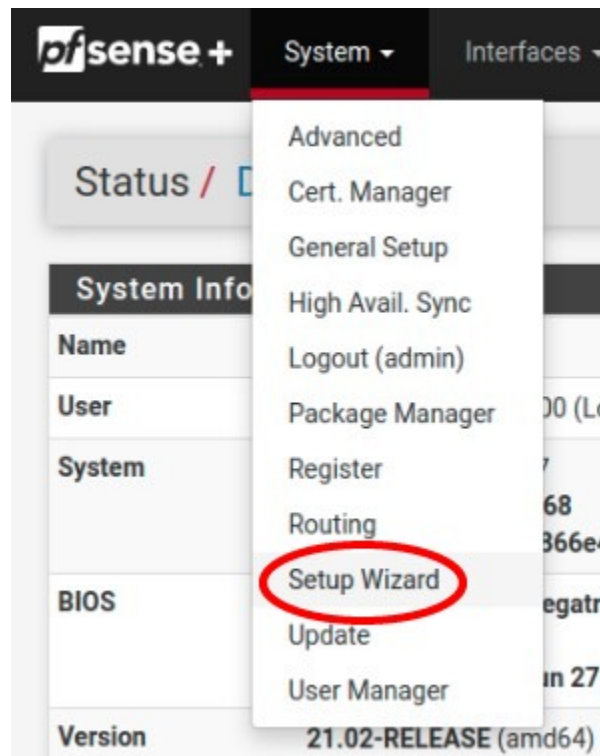


Fig. 9: Re-run the Setup Wizard

1.3.3 Backup and Restore

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

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

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

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

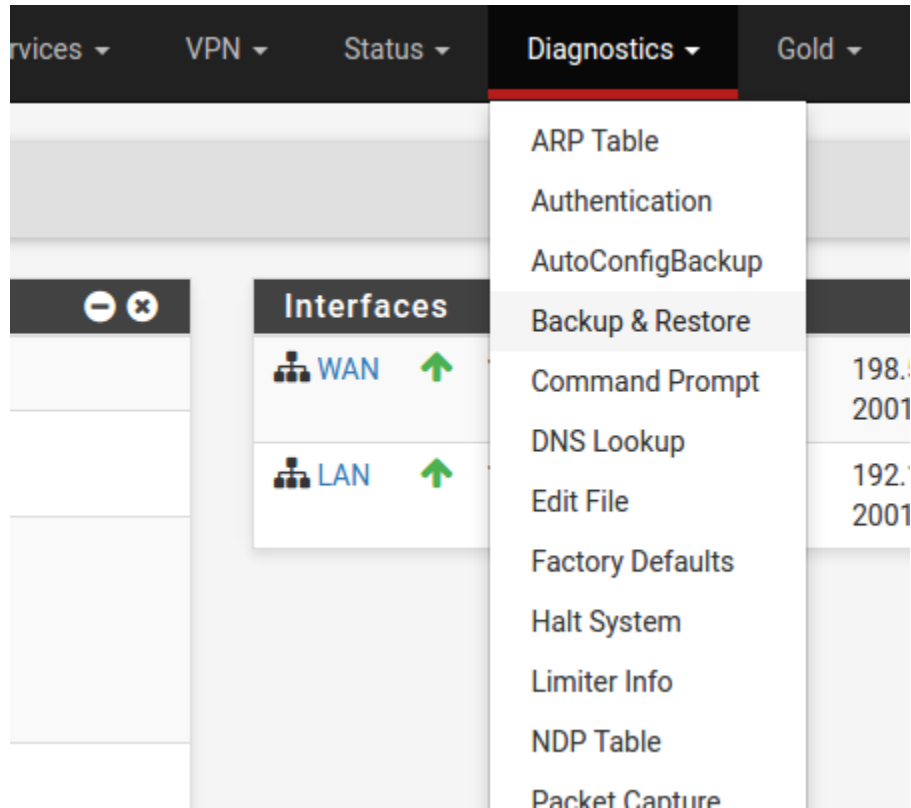


Fig. 10: Backup & Restore

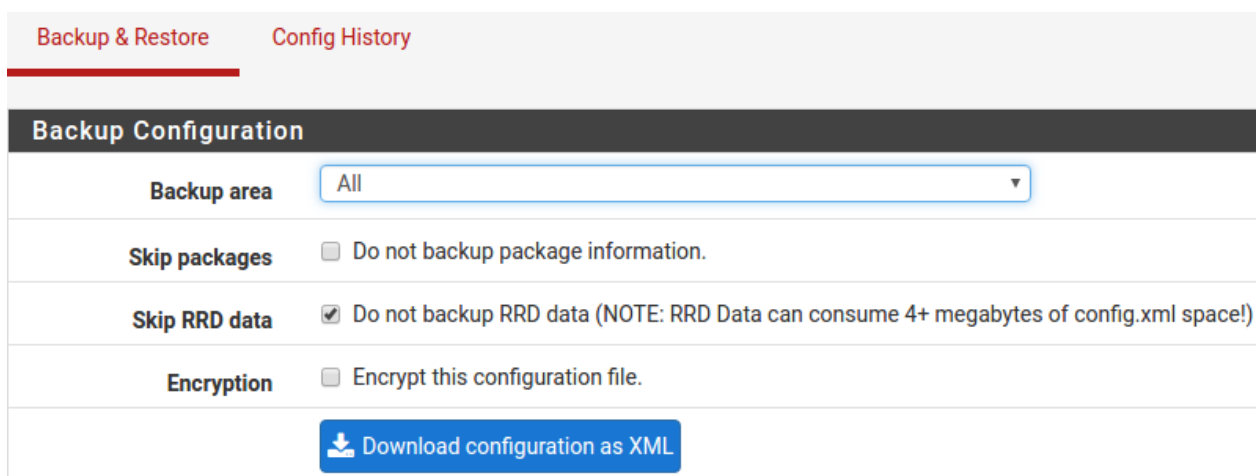


Fig. 11: Click Download configuration as XML

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 Console Port. Cable is required.

Tip: To learn more about getting the most out of a Netgate appliance, sign up for a [pfSense Plus Software Training](#) course or browse the extensive [Resource Library](#).

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

1.4.1 Front Panel

The front panel of the Netgate 8300 contains several items of interest for connecting to and managing the device.

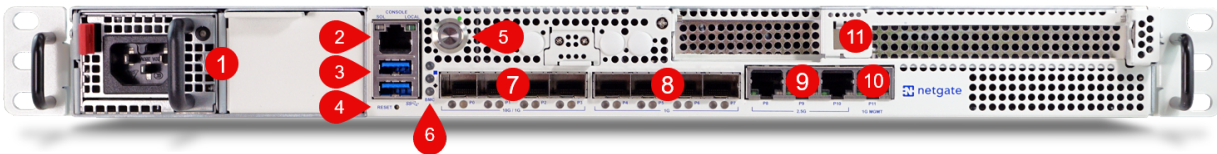


Fig. 12: Front view of the Netgate 8300 Security Gateway with key items numbered

The items below are marked with numbers on figure *Front view of the Netgate 8300 Security Gateway with key items numbered*:

Item	Description
1	Power Supply Unit (PSU) Bays
2	Serial Console (<i>RJ45</i>)
3	2x USB 3.0 Port
4	Reset Button – Used when performing the <i>Factory Reset Procedure</i> .
5	ACPI Power Button - Graceful shutdown, hard power off (Hold 10s), power on
6	<i>Status LEDs</i>
7	10G/1G SFP+ <i>Networking Ports</i>
8	1G SFP <i>Networking Ports</i>
9	2.5G RJ45 <i>Networking Ports</i>
10	1G IPMI Management Port (P11, <i>Intelligent Platform Management Interface (IPMI)</i>)
11	Add-on Expansion Card Slots

Power Supply Unit (PSU) Bays (1)

The chassis contains two power supply unit bays located on the far left of the front side. The PSUs are hot swappable and the unit can operate with one or both PSUs connected to line power.

The Netgate 8300 BASE unit ships with one power supply, the Netgate 8300 MAX unit ships with dual power supplies. Additional power supplies are available. A second PSU can be added to the BASE model later by removing the blank panel cover.

Each PSU is 500W with 110V/240V AC input. It contains a standard IEC320-C16 (3-pin) power receptacle which accepts a standard IEC320-C15 power plug.

Serial Console Port (2)

Clients can access the serial console using the [RJ45](#) “Cisco” style console port with a separate cable and USB serial adapter or client hardware port.

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

2x USB 3.0 Ports (3)

USB ports on the device can be used for a variety of purposes.

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

Reset Button (4)

The Reset Button is used to perform the [Factory Reset Procedure](#).

Pressing and immediately releasing the button has no effect, it does not perform a hardware reset.

See [Factory Reset Procedure](#) for details on how to use the button to perform a factory reset.

ACPI Power Button (5)

The large round lighted Power Button behaves the same as a typical ACPI power button.

If the device is powered on and running, pressing the button immediately performs a graceful shutdown and the system enters a standby state.

If the system is in a powered off or standby state, pressing the power button immediately powers on the device and starts the boot process.

If the system is unresponsive, holding in the power button for 10 seconds will forcefully power off the device. Press the power button again to turn it back on.

Status LEDs (6)

The status LEDs, including the backlight on the power button, indicate various status information for the device. The power button LED and the first two LEDs from top to bottom are for OS status, while the bottom LED is for the status of the baseboard management controller (BMC).

See [Status LEDs](#) for information on interpreting the meaning of different LED states.

10G/1G SFP+ Networking Ports (7)

This group of four ports labeled P0-P3 are [10G/1G SFP+ Networking Ports](#).

1G SFP Networking Ports (8)

This group of four ports labeled P4-P7 are [1G SFP Networking Ports](#).

2.5G RJ45 Networking Ports (9)

This group of three ports labeled P8-P10 are [2.5G RJ45 Networking Ports](#).

1G IPMI Management Port (10)

The rightmost RJ45 port labeled P11 is the 1G MGMT port dedicated to IPMI. See *Intelligent Platform Management Interface (IPMI)* for details on how to access IPMI.

Note: This dedicated IPMI management port is not visible to or usable by the operating system.

Add-on Expansion Card Slots (11)

These are expansion slots and covers which may house additional add-on cards such as for network interfaces. See *Add-On Expansion Card Installation* for installation information.

There are two available expansion slots:

- 1x PCIe 3.0 x8 LP (Low Profile) slot which supports half-length low profile cards.

This slot has a PCIe-LP connector which is PCIe x16 but only wired for PCIe x8. While the slot supports PCIe x16 half length cards, only 8 lanes function.

- 1x PCIe 4.0 x16 slot which supports full-height three-quarter length cards.

This x16 PCIe slot can supply a maximum of 75W directly.

Note: The power draw of standard 25-100 Gbit/s network interface cards will NOT exceed the standard 75W slot rating.

Networking Ports

The sections on the front of the device numbered **7**, **8**, and **9** in *Front view of the Netgate 8300 Security Gateway with key items numbered* contain the network interfaces. These ports are labeled **P0** through **P10** on the device and are grouped by speed.

Label	Assigned Name	Device Name	Type	Speed
P0	P0	ice0	SFP+	10 Gbps/1 Gbps
P1	P1	ice1	SFP+	10 Gbps/1 Gbps
P2	P2	ice2	SFP+	10 Gbps/1 Gbps
P3	P3	ice3	SFP+	10 Gbps/1 Gbps
P4	P4	ice4	SFP	1 Gbps
P5	P5	ice5	SFP	1 Gbps
P6	P6	ice6	SFP	1 Gbps
P7	P7	ice7	SFP	1 Gbps
P8	P8	igc2	RJ45	2.5 Gbps
P9	P9LAN	igc1	RJ45	2.5 Gbps
P10	P10WAN	igc0	RJ45	2.5 Gbps

Note: Network ports in add-on cards may shift the device names in the operating system however the default assignments still attempt match the assigned names with the labels on the device.

Note: The igc(4) network interfaces on this device **do not** support fixed speed operation. These interfaces emulate a speed/duplex choice by limiting the values offered during autonegotiation to the speed/duplex value selected in the GUI.

When connecting different devices to these interfaces the peer should typically be set to autonegotiate, not to a specific speed or duplex value. The exception to this is if the peer interface has the same limitation, in which case both peers should select the same negotiation speed.

Networking Ports with Add-on Cards

The current add-on network cards offered by Netgate all utilize the `ice(4)` driver regardless of speed and port type. These cards also all contain two ports each. The add-on cards get probed before the on-board ports, shifting the OS device names of the on-board ports. The default interface assignment code takes this into account when the cards are present on new/fresh installations and after a factory reset.

Warning: Adding an add-on card utilizing the `ice(4)` driver to an existing installation will cause the port assignments to be incorrect and may result in the WAN, LAN, and other ports being assigned to different physical interfaces.

There are two add-on expansion card slots on the Netgate 8300 device and they can both be populated with network cards, for a total of either two or four additional network ports.

The following table shows the default interface assignments for a Netgate 8300 containing a single two-port add-on card using the `ice(4)` driver:

Table 1: Interface assignments with a single two-port `ice(4)` add-on card

Label	Assigned Name	Device Name	Type	Speed
P0	P0	ice2	SFP+	10 Gbps/1 Gbps
P1	P1	ice3	SFP+	10 Gbps/1 Gbps
P2	P2	ice4	SFP+	10 Gbps/1 Gbps
P3	P3	ice5	SFP+	10 Gbps/1 Gbps
P4	P4	ice6	SFP	1 Gbps
P5	P5	ice7	SFP	1 Gbps
P6	P6	ice8	SFP	1 Gbps
P7	P7	ice9	SFP	1 Gbps
P8	P8	igc2	RJ45	2.5 Gbps
P9	P9LAN	igc1	RJ45	2.5 Gbps
P10	P10WAN	igc0	RJ45	2.5 Gbps
n/a	ADDON0	ice0	Varies	Varies
n/a	ADDON1	ice1	Varies	Varies

The following table shows the default interface assignments for a Netgate 8300 containing two two-port add-on cards using the `ice(4)` driver:

Table 2: Interface assignments with two two-port ice(4) add-on cards

Label	Assigned Name	Device Name	Type	Speed
P0	P0	ice4	SFP+	10 Gbps/1 Gbps
P1	P1	ice5	SFP+	10 Gbps/1 Gbps
P2	P2	ice6	SFP+	10 Gbps/1 Gbps
P3	P3	ice7	SFP+	10 Gbps/1 Gbps
P4	P4	ice8	SFP	1 Gbps
P5	P5	ice9	SFP	1 Gbps
P6	P6	ice10	SFP	1 Gbps
P7	P7	ice11	SFP	1 Gbps
P8	P8	igc2	RJ45	2.5 Gbps
P9	P9LAN	igc1	RJ45	2.5 Gbps
P10	P10WAN	igc0	RJ45	2.5 Gbps
n/a	ADDON0	ice0	Varies	Varies
n/a	ADDON1	ice1	Varies	Varies
n/a	ADDON2	ice2	Varies	Varies
n/a	ADDON3	ice3	Varies	Varies

Note: Cards utilizing different drivers may function in the add-on slots, but they will not be automatically assigned as interfaces by default.

1.4.2 Status LEDs

The Netgate 8300 has two groups of status LEDs: Three LEDs (including the power button) for the operating system status, and one LED for the baseboard management controller (BMC) status.

The Operating System status LEDs are labeled with shapes which correspond to each LED: Green Circle, Blue Square, and Black Diamond. The BMC status LED is labeled “BMC”.

OS Status LED Patterns

Description	LED Pattern
Standby	Circle pulsing amber
Power Applied	Circle solid amber
BIOS Booting	Circle flashing green
OS Kernel Booting	Circle solid green
OS Boot in Process	Circle flashing green, Square and Diamond flashing blue
Boot Completed/Ready	Circle solid green
Upgrade Available	Square solid amber
Upgrade in Progress	All flashing green
Triggering Reset	Circle, Square, then Diamond solid amber (<i>Factory Reset Procedure</i>)
Reset In Progress	All flashing amber (<i>Factory Reset Procedure</i>)

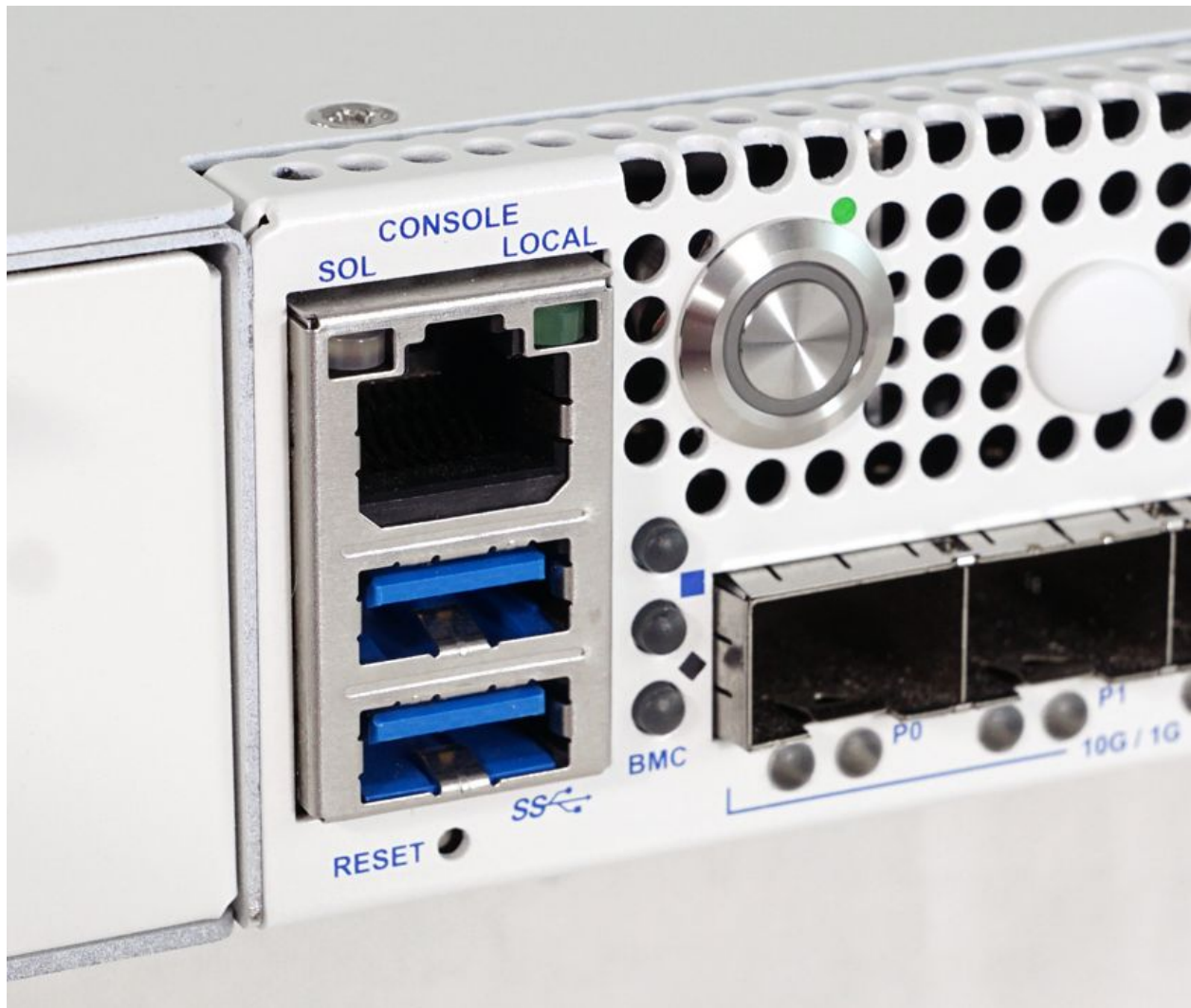


Fig. 13: Close-up view of the Netgate 8300 Security Gateway Status LEDs

BMC Status LED Patterns

Description	LED Pattern
BMC Power Applied	BMC solid amber
BMC OS Booting	BMC flashing blue
BMC Boot Completed/Ready	BMC solid blue

Power Supply Unit LED Patterns

Each power supply has a status LED in the upper right corner (not pictured).

Description	LED Pattern
Power Applied + Power On	PSU solid green
Power Applied + Power Off	PSU flashing green
Power Loss to all PSUs	PSU off
Power Loss to one PSU ¹	PSU flashing amber
Warning Event ²	PSU flashing alternating amber and green
Critical Event ³	PSU solid amber

PSU LED Notes

1.4.3 Rear Panel

The rear panel of the device has items which are not meant to be accessed as often as the front, as the device is intended to be mounted in a rack.



Fig. 14: Rear view of the Netgate 8300 Security Gateway with key items numbered

The items below are marked with numbers on figure *Rear view of the Netgate 8300 Security Gateway with key items numbered*:

Item	Description
1	Fan exhaust grills
2	Ground connection
3	Power switch

¹ When multiple PSUs are installed.

² PSU continues operating during warning events. Warning events include: High temperature, power level higher than expected, current higher than expected, fan operating slower than expected.

³ Critical events cause a PSU to shut down. Critical events include: PSU failure, output over current protection, output over voltage protection, fan failure.

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 A 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 commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operations of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

1.5.4 Industry Canada

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

1.5.5 Australia and New Zealand

This is an EMC Compliance level 2 product. This product is suitable for domestic environments.

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

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

Dansk [Danish]

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

Nederlands [Dutch]

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

English

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

Eesti [Estonian]

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

Suomi [Finnish]

NETGATE vakuuttaa täten että NETGATE device, tyypinen 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". (BMW i)

Ελληνικά [Greek]

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

Magyar [Hungarian]

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

Íslenska [Icelandic]

Hér me l sír NETGATE yfir ví a NETGATE device, er í samræmi við 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 ijjiet essenzjali u ma provvedimenti o rajn rilevanti 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 týmto vyhlasuje, že NETGATE device, spĺňa základné požiadavky a všetky príslušné 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 oświadcza, że 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 Connecting to the 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.

There are multiple ways to access the console on the **Netgate 8300**:

- IPMI Web Browser Serial Console
- Serial over LAN (SOL) via `ipmitool`
- Using the RJ45 hardware console port

Warning: Only **one** console method can be utilized at a time. Connecting a client to one console type will cause the other access methods to behave erratically.

2.1.1 Connecting to IPMI Web Browser Serial Console

The IPMI interface on the **Netgate 8300** contains a web-based serial console accessible via browser. This client is HTML-based and does not require extra software, only a current web browser.

To access the console:

- Log into the IPMI web interface as described in *Intelligent Platform Management Interface (IPMI)*
- Navigate to **Remote Control > SOL**

2.1.2 Connecting to IPMI Serial-over-LAN Console

The IPMI Serial-over-LAN (SOL) console can also be accessed via IPMI utilities such as `ipmiconsole` which is included with `ipmitool`.

To access the SOL console using `ipmiconsole`, first install `ipmitool` on the client and then run the following command:

```
$ ipmiconsole -h <address> -u <user> -P
```

Replace `<address>` with the IP address or hostname of the IPMI interface.

Replace `<user>` with a valid IPMI user with sufficient privileges to access SOL.

The `-P` parameter causes `ipmiconsole` to prompt for a password.

2.1.3 Connecting to RJ45 Console Port

A separate adapter is required to make a connection between a computer and the firewall using the RJ45 serial port. The **Netgate 8300** device ships with a USB A to RJ45 console cable suitable for this purpose, which is covered in the next section.



Fig. 1: Serial cable connected to RJ45 Console Port

Any compatible cable may be used instead of the one shipped with the device. 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.

2.1.4 Using the Supplied USB A to RJ45 Serial Adapter

The supplied USB A to RJ45 serial adapter cable contains a **Prolific PL2303GT USB-to-UART Bridge** which can be used to access the console.

Install the Driver

If needed, install an appropriate **Prolific PL2303GT 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](#).

Linux

There are drivers available for Linux [available for download](#).

Recent versions of many Linux distributions include this driver and will not require manual installation.

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 **RJ-45** connector on one end and a **USB Type A** plug on the other end.

Gently push the **RJ-45** 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 **RJ-45** 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.

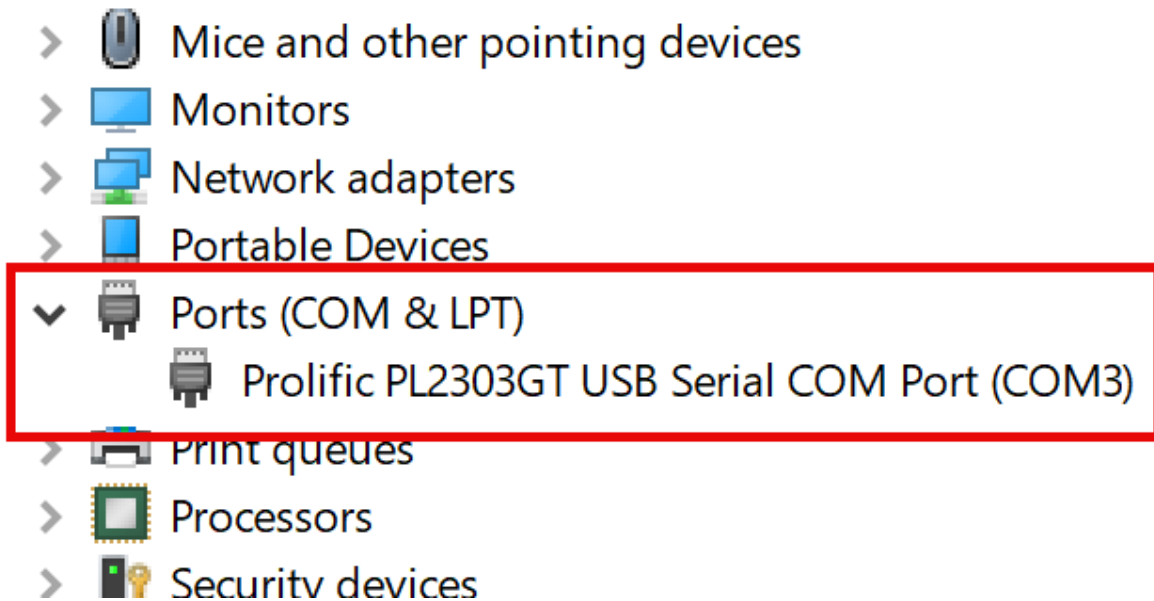
Locate the Console Port Device

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 **Prolific PL2303GT USB Serial COM Port**. 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/tty.PL2303G-USBtoUART<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.

2.1.5 Launch a Terminal Program

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

Windows

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

Warning: Do not use **Hyperterminal**.

macOS

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

Linux

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

FreeBSD

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

Client-Specific Examples

PuTTY in Windows

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

PuTTY will then display the console.

PuTTY in Linux

- Open PuTTY from a terminal by typing `sudo putty`

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

- Set the **Connection type** to **Serial**
- Set **Serial line** to `/dev/ttyUSB0`
- Set the **Speed** to 115200 bits per second

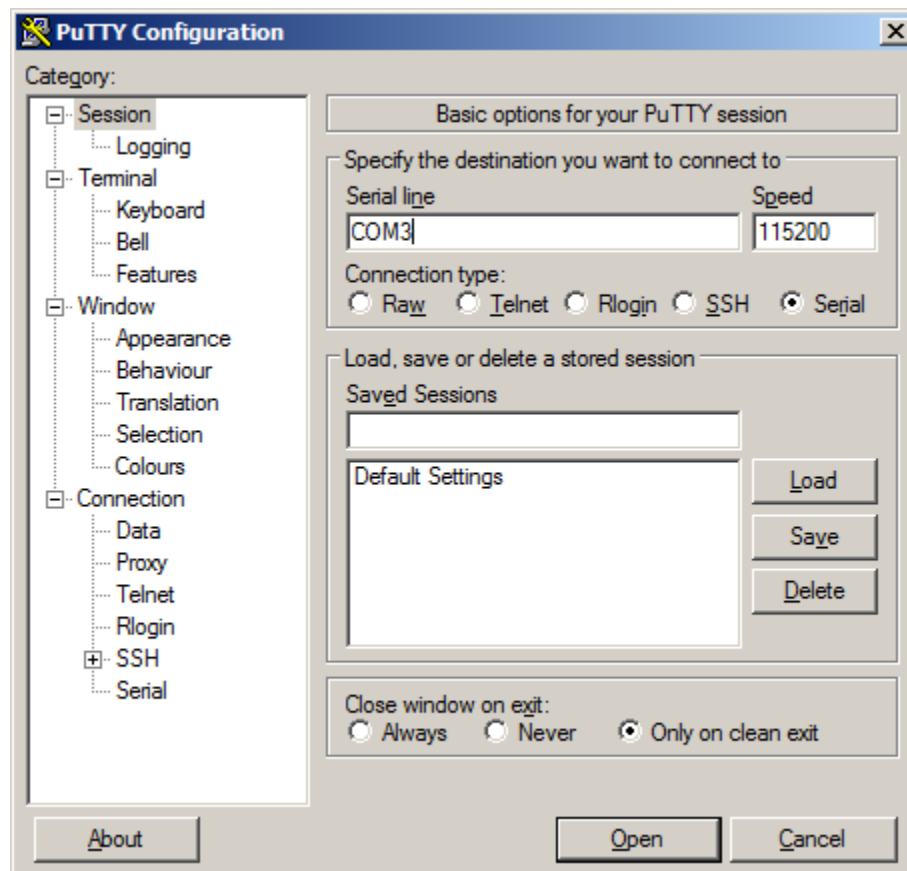


Fig. 2: An example of using PuTTY in Windows

- Click the **Open** button

PuTTY will then display the console.

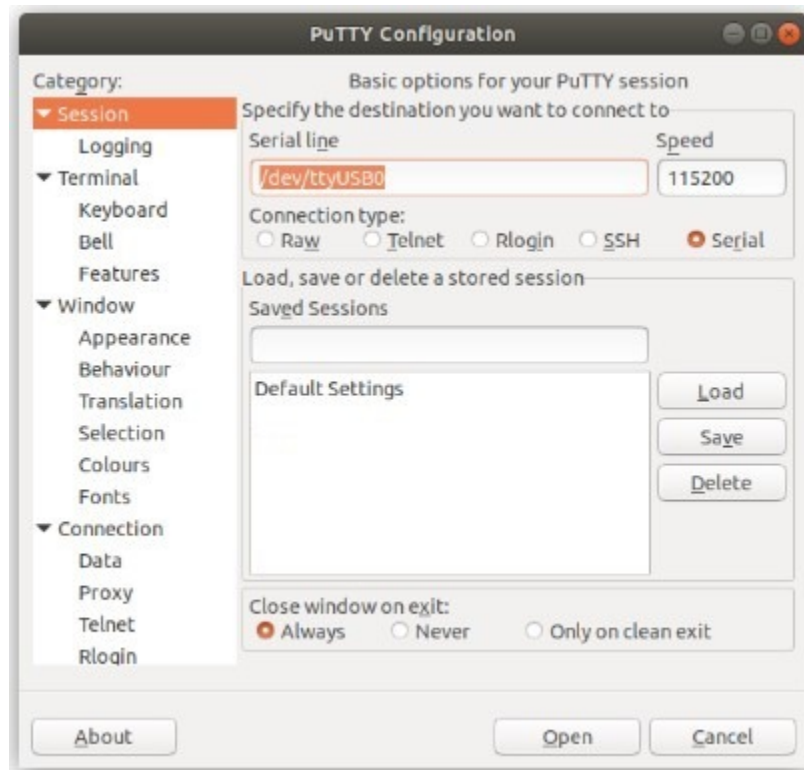


Fig. 3: An example of using PuTTY in Linux

GNU screen

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

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

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

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

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

Terminal Settings

The settings to use within the terminal program are:

Speed

115200 baud, the speed of the BIOS

Data bits

8

Parity

None

Stop bits

1

Flow Control

Off or XON/OFF.

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

Terminal Optimization

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

These are:

Terminal Type

xterm

This setting may be under Terminal, Terminal Emulation, or similar areas.

Color Support

ANSI colors / 256 Color / ANSI with 256 Colors

This setting may be under Terminal Emulation, Window Colors, Text, Advanced Terminfo, or similar areas.

Character Set / Character Encoding

UTF-8

This setting may be under Terminal Appearance, Window Translation, Advanced International, or similar areas. In GNU screen this is activated by passing the -U parameter.

Line Drawing

Look for and enable setting such as “Draw lines graphically”, “Use unicode graphics characters”, and/or “Use Unicode line drawing code points”.

These settings may be under Terminal Appearance, Window Translation, or similar areas.

Function Keys / Keypad

Xterm R6

In Putty this is under **Terminal > Keyboard** and is labeled **The Function Keys and Keypad**.

Font

For the best experience, use a modern monospace unicode font such as Deja Vu Sans Mono, Liberation Mono, Monaco, Consolas, Fira Code, or similar.

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

2.1.6 What's Next?

After connecting a terminal client, it may not immediately see any output. This could be because the device has already finished booting or it may be that the device is waiting for some other input.

If the device does not yet have power applied, plug it in and monitor the terminal output.

If the device is already powered on, try pressing **Space**. If there is still no output, press **Enter**. If the device was booted, it may redisplay the console menu or login prompt, or produce other output indicating its status.

From the console, a variety of things are possible, such as changing interface addresses. There is a [full explanation of every console menu option in the pfSense software documentation](#).

2.1.7 Troubleshooting

Serial Device Missing

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

No Power

Some models require power before the client can connect to the USB serial console.

USB Cable Not Plugged In

For USB consoles, the USB cable may not be fully engaged on both ends. Gently, but firmly, ensure the cable has a good connection on both sides.

Bad USB Cable

Some USB cables are not suitable for use as data cables. For example, some cables are only capable of delivering power for charging devices and not acting as data cables. Others may be of low quality or have poor or worn connectors.

The ideal cable to use is the one that came with the device. Failing that, ensure the cable is of the correct type and specifications, and try multiple cables.

Wrong Device

In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.

Hardware Failure

There could be a hardware failure preventing the serial console from working. Contact Netgate TAC for assistance.

No Serial Output

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

USB Cable Not Plugged In

For USB consoles, the USB cable may not be fully engaged on both ends. Gently, but firmly, ensure the cable has a good connection on both sides.

Wrong Device

In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.

Wrong Terminal Settings

Ensure the terminal program is configured for the correct speed. The default BIOS speed is 115200, and many other modern operating systems use that speed as well.

Some older operating systems or custom configurations may use slower speeds such as 9600 or 38400.

Device OS Serial Console Settings

Ensure the operating system is configured for the proper console (e.g. `ttys1` in Linux). Consult the various operating install guides on this site for further information.

PuTTY has issues with line drawing

PuTTY generally handles most cases OK but can have issues with line drawing characters on certain platforms.

These settings seem to work best (tested on Windows):

Window

Columns x Rows
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 install guides on this site for further information.

Bootable Media

If booting from a USB flash drive, ensure that the drive was written correctly and contains a bootable operating system image.

2.2 Intelligent Platform Management Interface (IPMI)

The **Netgate 8300** appliance includes a baseboard management controller (BMC) for out-of-band (OOB) access via Intelligent Platform Management Interface (IPMI). Administrators can use this interface to control the hardware itself, such as power on/off, access a serial over LAN (SOL) console, mount virtual media for installation, see hardware status events, and more.

IPMI Usage Topics

- [Accessing IPMI](#)
- [Default IPMI Credentials](#)
- [IPMI Password Requirements](#)
- [Changing the IPMI Password](#)
- [Reset IPMI Network Configuration](#)
- [Factory Reset the BMC](#)
- [Re-arm the Chassis Intrusion Switch](#)

2.2.1 Accessing IPMI

To access IPMI via its web-based GUI, navigate to the IP address of the BMC using a web browser, e.g. `https://10.10.10.89`. It can also be accessed using [ipmitool](#) over the network.

By default, the dedicated IPMI network port (**P11**) is configured to be a DHCP client but it can be manually configured with a static address.

The address of the BMC set to DHCP can be determined in a few different ways:

- Enter the BIOS when powering on the device and navigate to **Server Mgmt > BMC Network Configuration**. That screen displays the current network information for the BMC.
- From the installed Operating System, run `ipmitool lan print 2` to output the current BMC/IPMI network configuration for the dedicated IPMI network port.

- Check the DHCP server leases to see which lease was allocated to the BMC.

Tip: The MAC address of the BMC is printed on the device label for reference.

2.2.2 Default IPMI Credentials

The default IPMI username is **root** and the default password is **root**.

In compliance with privacy legislation, the Username and Password to access the IPMI port on the **Netgate 8300** **must be changed** on first access.

The IPMI web interface will present a screen to change the password immediately upon the first login using the default credentials.

To change the password:

- Navigate to the IPMI address using a web browser
- Log in to the IPMI Web Console with the default credentials.
- Enter the following items on the **Change Password** form:

Old Password

The current default password (**root**).

New Password

The new password to set. If the password is acceptable, the field will be outlined in green. If the password is invalid, the field will be outlined in red.

See also:

For a list of password requirements, see the next section. The IPMI Web Console will also print the requirements if a user attempts to set a password it considers too weak.

Confirm Password

The same password as in the **New Password** field. If the passwords match, the field will be outlined in green. If the passwords do not match, the field will be outlined in red.

- Click **Update Password**

2.2.3 IPMI Password Requirements

IPMI user account passwords must meet the following criteria:

- Minimum of 6 characters long
- Contains only printable ASCII characters
- Cannot contain the account name (Case insensitive)
- Meets at least 3 of following criteria:
 - Contains uppercase characters (A through Z)
 - Contains lowercase characters (a through z)
 - Contains numbers (0 through 9)
 - Contains special characters (e.g., \$, &)

Change Password

Password should be changed for default user and should have a minimum of 8 characters.

Username

root

Old password

👁

New password ⓘ

👁

Confirm new password

👁

Update Password

© 2013-2022 Insyde Software Corp.

Fig. 4: IPMI Web Console forcing a password change on first login

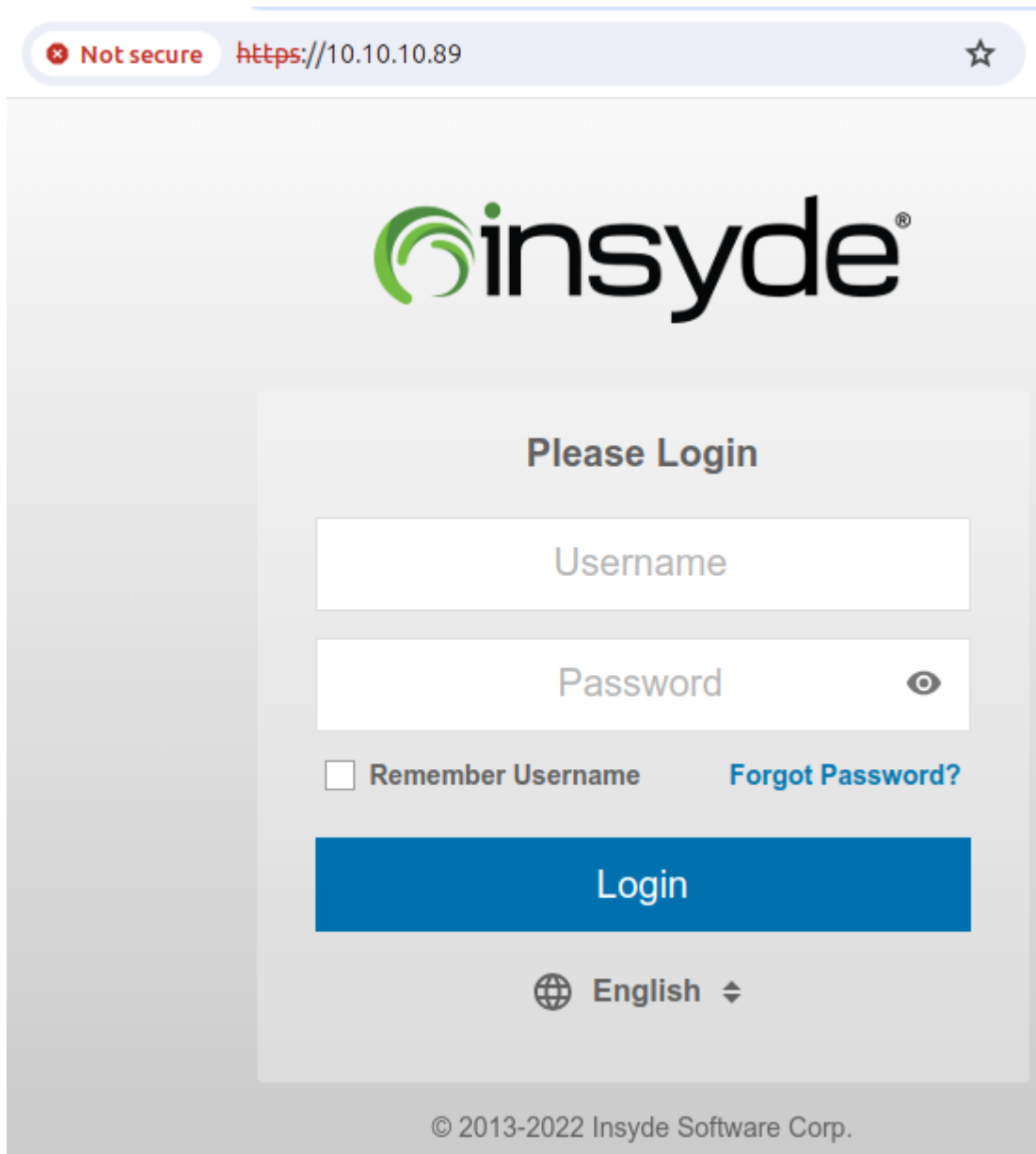
2.2.4 Changing the IPMI Password

The IPMI password for **Netgate 8300** appliances can be changed either through the browser-based IPMI console or by using the `ipmitool` utility directly in pfSense® software.

Using IPMI Web Console

To change the IPMI password in the web console:

- Navigate to the IPMI address using a web browser
- Log in to the IPMI console with the current credentials



The screenshot shows a web browser window with the address bar displaying "https://10.10.10.89". The browser indicates the connection is "Not secure". The main content area features the "insyde" logo at the top. Below the logo is a "Please Login" section containing a "Username" input field, a "Password" input field with a toggle eye icon, a "Remember Username" checkbox, and a "Forgot Password?" link. A large blue "Login" button is positioned below these fields. At the bottom of the login section is a language selector showing "English" with a globe icon and a dropdown arrow. The footer of the page reads "© 2013-2022 Insyde Software Corp."

Fig. 5: Log Into IPMI

Note: If the username is not known, see the next section for information on how to use `ipmitool` to view the current user list.

- Navigate to **Configuration > Users**

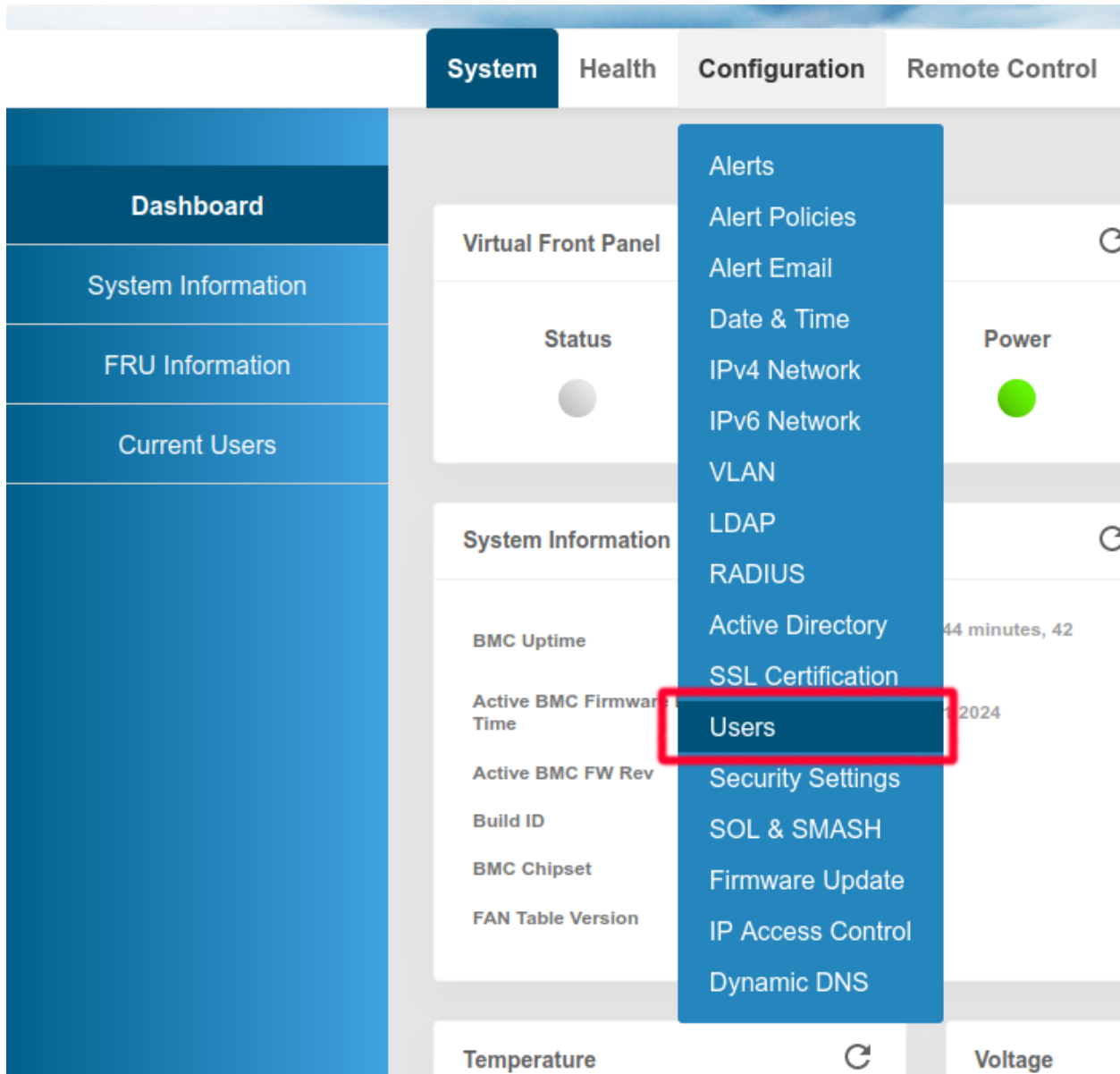


Fig. 6: Configuration > Users

- Select the user to modify by clicking on its row in the list

This is likely the root user or another user with *Administrator* privileges, typically the user in the second slot (User ID 2).

- Click **Modify User**
- Set the form fields as follows:

User ID	User Name	User Status	Network Privilege	SOL Payload Access	SNMPv3 Access	IPMI Messaging	Email
1	anonymous	Disable	No Access	Disable	Disable	Disable	
2	root	Enable	Administrator	Enable	Disable	Enable	
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

Add User
Modify User
Delete User

Fig. 7: Modify User

User Name

Change the username from the default **root** to a personalized name

This is optional, but a best practice.

Change Password

Click to enable the slider

Password

Enter the new **Password**

If the password is acceptable, the field will be outlined in green. If the password is invalid, the field will be outlined in red.

See also:

For a list of password requirements, see the previous section.

Confirm Password

Enter the new password again in **Confirm Password**

If the passwords match, the field will be outlined in green. If the passwords do not match, the field will be outlined in red.

- Click **Modify**
- Click **Confirm** on the alert that says “Modified user successfully.”

Using the ipmitool Utility

If the IPMI web interface is unavailable or the current password is unknown, the **ipmitool** utility packaged with pfSense software can change the password.

These commands may be performed in the GUI at **Diagnostics > Command Prompt** or at a console or SSH shell prompt as the root user.

- Load the IPMI kernel module

```
# kldload ipmi
```







User Name :	<input type="text" value="myuser"/>
Change Password :	<input checked="" type="checkbox"/> Change password will kill all current login session
Password :	<input type="password" value="....."/> 
Confirm Password :	<input type="password" value="....."/> 
Network Privileges :	<input type="text" value="Administrator"/> 
Email :	<input type="text" value="user@domain.com"/>
User Enable :	<input type="text" value="Enable"/> 
SOL Payload Access :	<input type="text" value="Enable"/> 
IPMI Messaging :	<input type="text" value="Enable"/> 

Fig. 8: Modify User Form

Success

Modified user successfully.

Confirm

Fig. 9: Click Confirm

- List the current IPMI users

```
# ipmitool user list
```

Note: Netgate 8300 appliances use the user name root by default.

The command prints a list of users, for example:

ID	Name	Callin	Link Auth	IPMI Msg	Channel Priv Limit
1		true	false	false	NO ACCESS
2	root	true	false	true	ADMINISTRATOR
3		true	false	false	NO ACCESS
4		true	false	false	NO ACCESS
5		true	false	false	NO ACCESS
6		true	false	false	NO ACCESS
7		true	false	false	NO ACCESS
8		true	false	false	NO ACCESS
9		true	false	false	NO ACCESS
10		true	false	false	NO ACCESS
11		true	false	false	NO ACCESS
12		true	false	false	NO ACCESS
13		true	false	false	NO ACCESS
14		true	false	false	NO ACCESS
15		true	false	false	NO ACCESS

Warning: Usernames are case-sensitive.

- Reset the password for a user

The default root user is User ID 2, and the example below sets the password for this user to NETGATE.

```
# ipmitool user set password 2 NETGATE
```

Warning: This password is for example purposes only. Use a secure password.

If successful, the output will be:

```
Set User Password command successful (user 2)
```

- Unload the IPMI kernel module

```
# kldunload ipmi
```

2.2.5 Reset IPMI Network Configuration

The `ipmitool` utility can also change or reset the network configuration of the IPMI interface if it cannot be reached over the network.

These commands may be performed in the GUI at **Diagnostics > Command Prompt** or at a console or SSH shell prompt as the `root` user.

Note: The dedicated IPMI port (**P11**) is on IPMI network channel **2**.

- Load the IPMI kernel module

```
# kldload ipmi
```

- Set the IPMI IP address and subnet mask

The following commands configure the IP address of the IPMI interface and its corresponding [subnet mask in dotted quad notation](#).

This example sets the IPMI IP address to `172.31.123.5/24`:

```
# ipmitool lan set 2 ipsrc static
# ipmitool lan set 2 ipaddr 172.31.123.5
# ipmitool lan set 2 netmask 255.255.255.0
```

- Set the IPMI gateway IP address

To communicate with IPMI outside of its configured subnet, the IPMI interface must have a default gateway set.

This example sets the default gateway to `172.31.123.1`.

```
# ipmitool lan set 2 defgw ipaddr 172.31.123.1
```

- Enable IPMI access on the interface

```
# ipmitool lan set 2 access on
```

- Unload the IPMI kernel module

```
# kldunload ipmi
```

2.2.6 Factory Reset the BMC

It is possible to factory reset the BMC configuration using `ipmitool` either locally or remotely. In certain cases this may help resolve problems accessing the BMC. For example, if the BMC GUI is inaccessible due to a configuration error or other problem. Performing a factory reset of the BMC will allow an administrator to access and reconfigure the BMC.

To factory reset the BMC, use the `ipmitool` utility. This can be performed locally from a running installation of pfSense software, or remotely from another system across the network.

Using ipmitool Locally

These commands may be performed in the GUI at **Diagnostics > Command Prompt** or at a console or SSH shell prompt as the root user.

- Load the IPMI kernel module

```
# kldload ipmi
```

- Factory reset the BMC

```
# ipmitool raw 0x30 0x02 0x43 0x4c 0x52 0xaa
# ipmitool raw 6 2
```

- Unload the IPMI kernel module

```
# kldunload ipmi
```

Using ipmitool Remotely

The remote BMC factory reset process requires the following items:

- The client system must have `ipmitool` installed.
- The BMC IP address.
- The BMC IP address must be reachable over the network from the client system.
- A valid username and password for the BMC with administrator access.

To factory reset the BMC remotely, use the following commands:

```
$ ipmitool -I lanplus -H <BMC_IP> -U <username> -P <password> raw 0x30 0x02 0x43 0x4c 0x52 0xaa
$ ipmitool -I lanplus -H <BMC_IP> -U <username> -P <password> raw 6 2
```

2.2.7 Re-arm the Chassis Intrusion Switch

The chassis on **Netgate 8300** has an intrusion detection function which can be reset via IPMI. See *Re-arm the Chassis Intrusion Switch* for details.

2.3 Updating the Baseboard Management Controller Firmware

Occasionally there are updates to the Baseboard Management Controller (BMC) firmware on the **Netgate 8300** to address problems or improve features. This firmware can be updated using the web interface on the BMC which also contains Intelligent Platform Management Interface (IPMI) functionality.

2.3.1 Warnings & Precautions

Warning: The firmware should only be updated at the direction of [Netgate TAC](#).

Warning: The device must be rebooted multiple times during this process. This reboots the BMC and the operating system, which will disrupt traffic passing through the device.

Warning: As a part of this update process the BMC may lose customizations made to the BMC settings and IPMI, including any network configuration, additional users, and any password changes. Make sure to note and custom settings and double check their values after completing the upgrade process.

2.3.2 Check the Firmware Version

Connect to the browser-based web interface on the BMC. To access this web interface, follow the directions in *Intelligent Platform Management Interface (IPMI)*.

Look for the **System Information** widget on the BMC GUI dashboard. In that box, there are three fields:

Active BMC Firmware Build Time

The time and date at which the current firmware was built.

Active BMC FW Rev

The current firmware revision.

Build ID

The build ID of the current firmware revision. This number roughly corresponds to the end of the firmware revision, but contains more digits at the end.

Note current values of both fields.

2.3.3 Obtain the Firmware Update File

Before starting, contact [Netgate TAC](#) and request the BMC firmware update file.

The firmware update file will have a name similar to `Netgate8300-BMC_FW-update-03.54.23.001101.bin` and may be compressed.

Compare the version in the filename to the current firmware revision and build ID noted earlier from the BMC GUI. The version number in the filename corresponds to the firmware revision and build ID reported in the BMC GUI.


If the firmware filename **matches** the current active BMC firmware revision, then it is already current and no update is necessary.

If the firmware filename contains a **newer** version than the current active BMC firmware revision, then proceed with the update.

The file should be on the same computer with the web browser being used to access the BMC web interface.

Note: If the firmware file is compressed, decompress it before proceeding.

System Information



BMC Uptime

19 hours, 10 minutes, 43 seconds

Active BMC Firmware Build Time

Fri Sep 13 04:06:19 2024

Active BMC FW Rev

03.54.23.0011

Build ID

23.001101

BMC Chipset

AST2620-A3

FAN Table Version

87.1.0

Fig. 10: Current active BMC firmware revision and build ID outlined in red

2.3.4 Update the Firmware

This update is performed in the browser-based web interface on the BMC. To access this web interface, follow the directions in *Intelligent Platform Management Interface (IPMI)*.

- Navigate to **Configuration > Firmware Update** in the web interface.
- Check **Reboot immediately after update**.

Warning: This reboots the BMC **and** the operating system.

- Click **Choose File**
- Select the firmware update file (e.g. Netgate8300-BMC_FW-update-03.54.23.001101.bin).
- Click **Upload** to start the upload process.
- Wait until the upload process is 100% complete.
- Click **Update** to start the BMC firmware update process.
- Wait for the update to complete and for the device to reboot.
- Log back into the BMC web interface.
- Verify the BMC version.

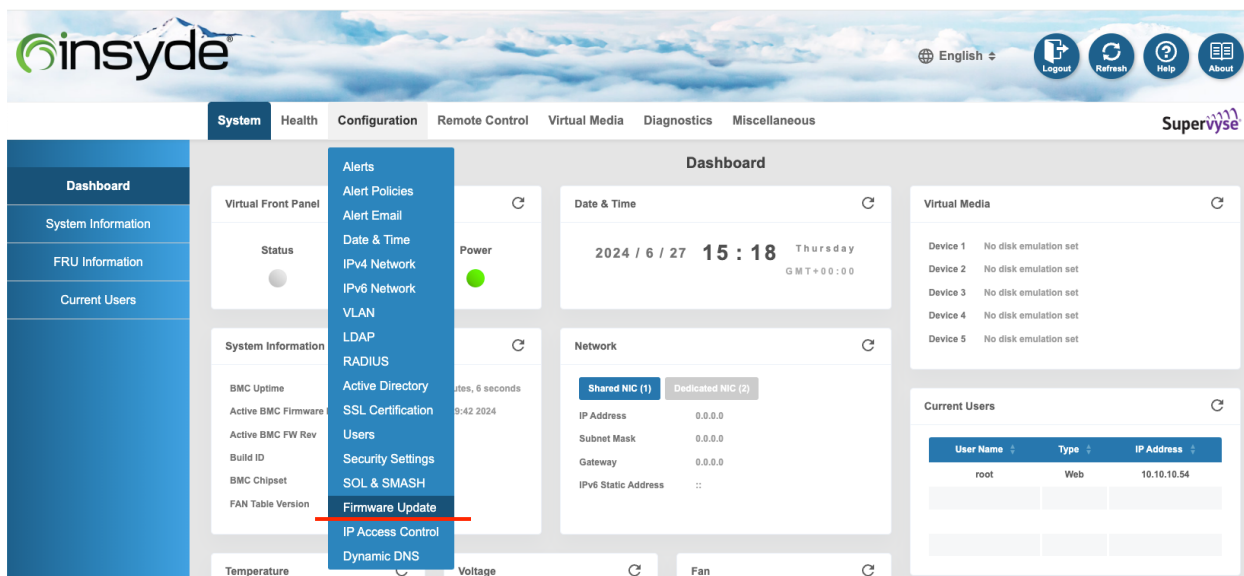


Fig. 11: Firmware Update menu location

Use this page to upload new BMC firmware.

☒ **Reboot immediately after update**

☐ Force update firmware

☐ Restore to default

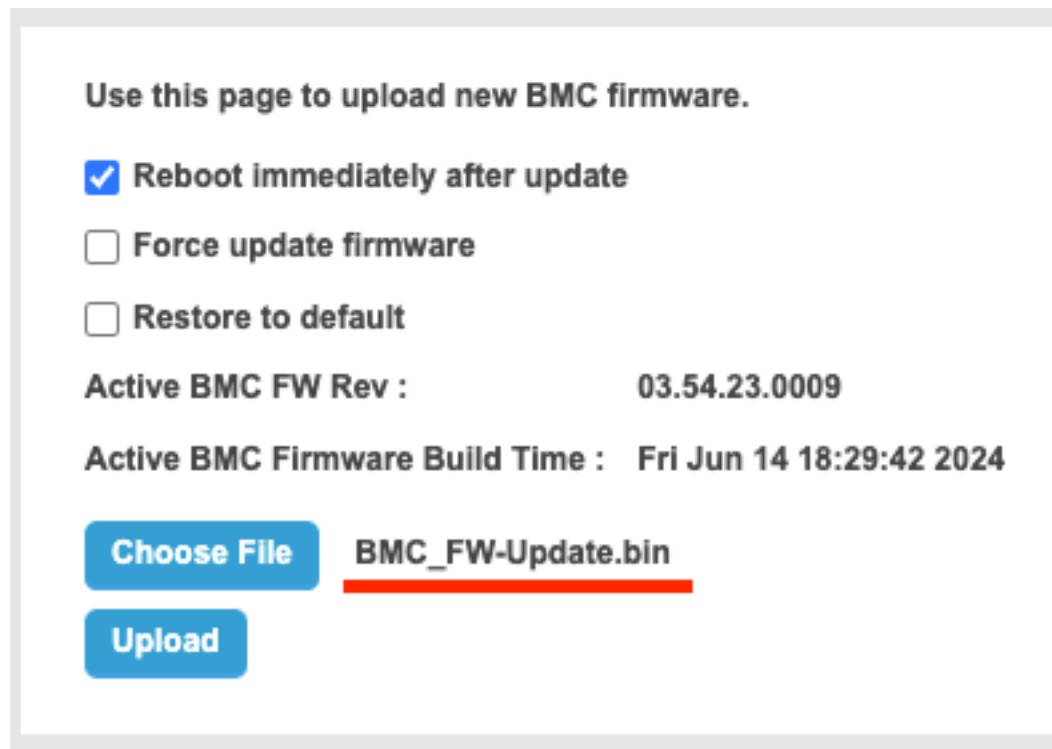
Active BMC FW Rev : 03.54.23.0009

Active BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

Choose File No file chosen

Upload

Fig. 12: Check the box to automatically reboot when the update finishes



Use this page to upload new BMC firmware.

☒ Reboot immediately after update

☐ Force update firmware

☐ Restore to default

Active BMC FW Rev : 03.54.23.0009

Active BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

Choose File BMC_FW-Update.bin

Upload

Fig. 13: Select the firmware update file (e.g. Netgate8300-BMC_FW-update-03.54.23.001101.bin)

2.3.5 Hardware Reset

To complete the update, the hardware must be undergo a cold boot, which can be performed via the BMC GUI as a hardware reset.

- Navigate to **Remote Control > Virtual Front Panel**.
- Select **Reset Host**
- Click **Perform Action** to reset the hardware and perform a cold boot.
- Wait for the device to boot.
- Log back into the BMC web interface and check all previous custom settings, making corrections if necessary.

2.4 Re-arm the Chassis Intrusion Switch

The chassis on **Netgate 8300** has an intrusion detection function. If the chassis has been opened the intrusion switch will be tripped even if the power was off.

Note: Chassis intrusion switch events and the current status of the sensor can be viewed in the IPMI web interface (*Intelligent Platform Management Interface (IPMI)*), but the only supported method to re-arm the sensor at this time is via IPMI CLI utilities.

Use this page to upload new BMC firmware.

☒ Reboot immediately after update

☐ Force update firmware

☐ Restore to default

Active BMC FW Rev : 03.54.23.0009

Active BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

BMC_FW-Update.bin

Upload firmware : 52%

Fig. 14: Firmware file upload in progress

Use this page to upload new BMC firmware.

☒ **Reboot immediately after update**

☐ **Force update firmware**

☐ **Restore to default**

Active BMC FW Rev : 03.54.23.0009

Active BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

Uploaded BMC FW Rev : 3.54.23

Uploaded BMC Firmware Build Time : Fri Jun 14 18:29:42 2024

Upload firmware : Done.

Authenticate firmware : Done.

Program firmware : 100%

Reboot BMC : Please wait while the BMC reboots to complete the update.

Fig. 15: Firmware update in progress

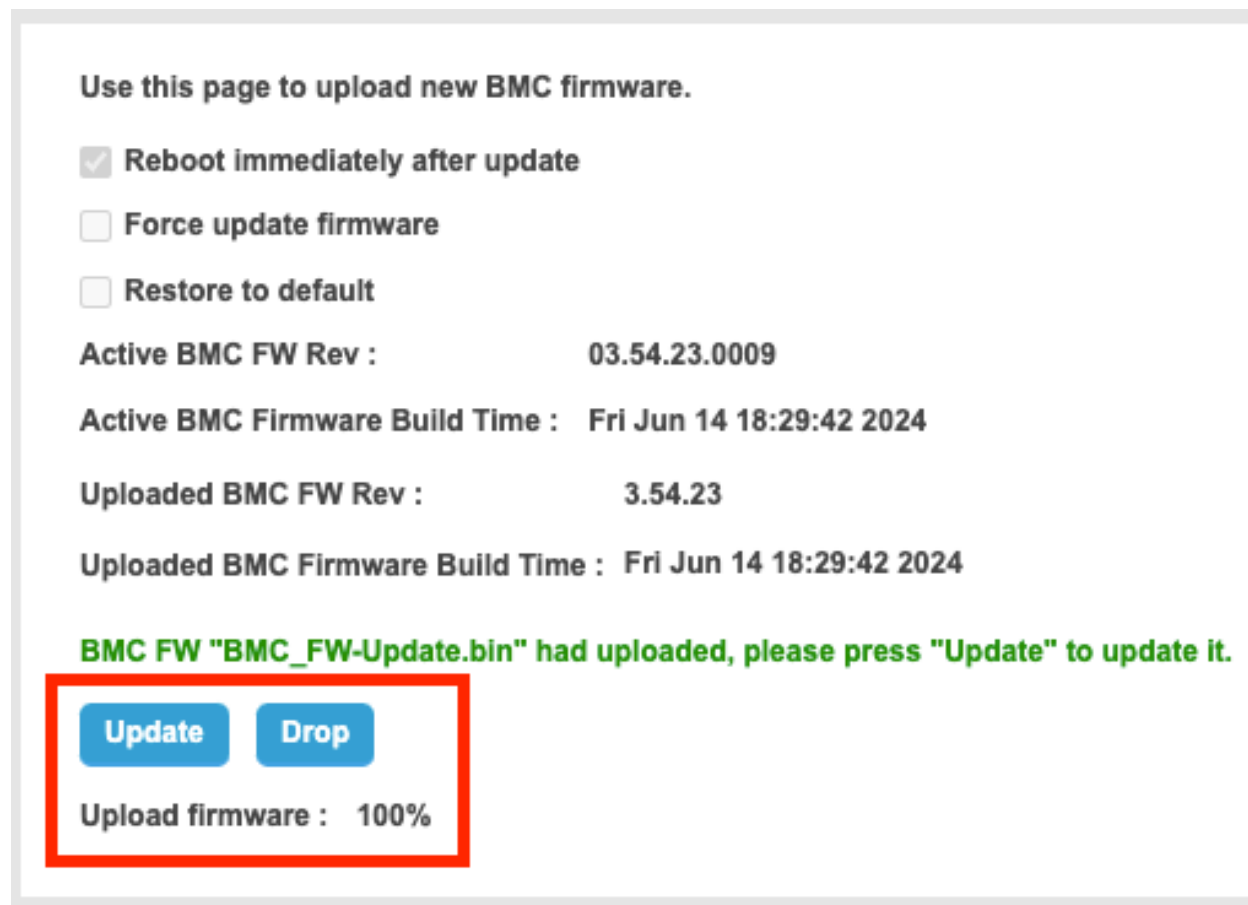
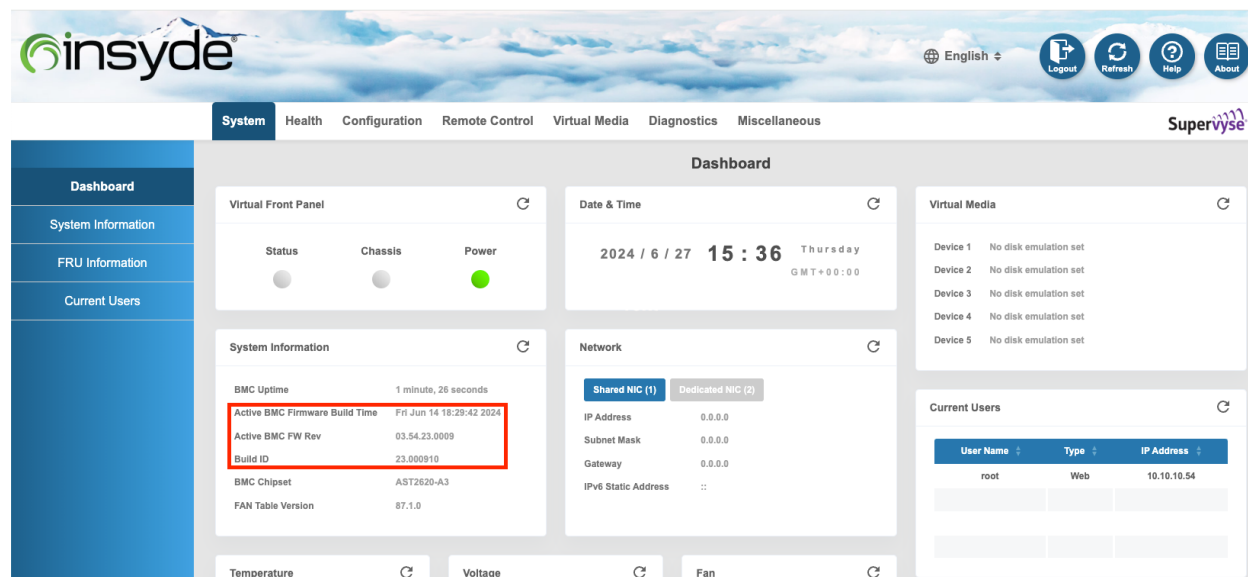
Fig. 16: Click **Update** to perform the firmware update

Fig. 17: Checking the BMC firmware version

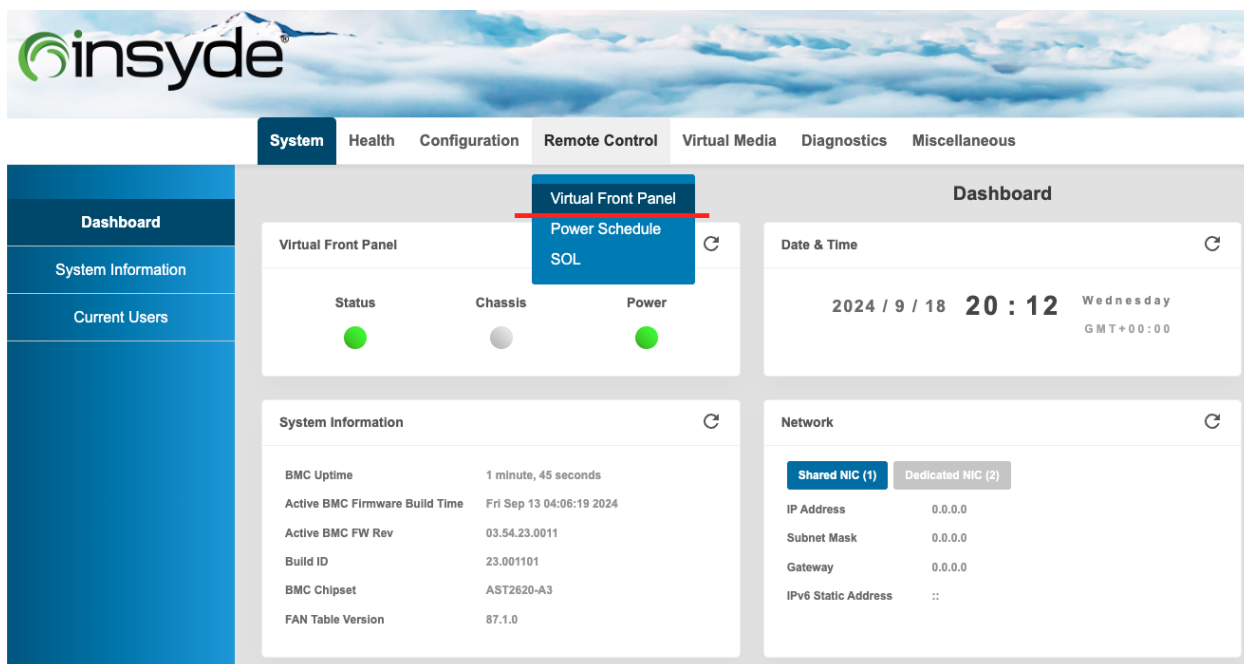
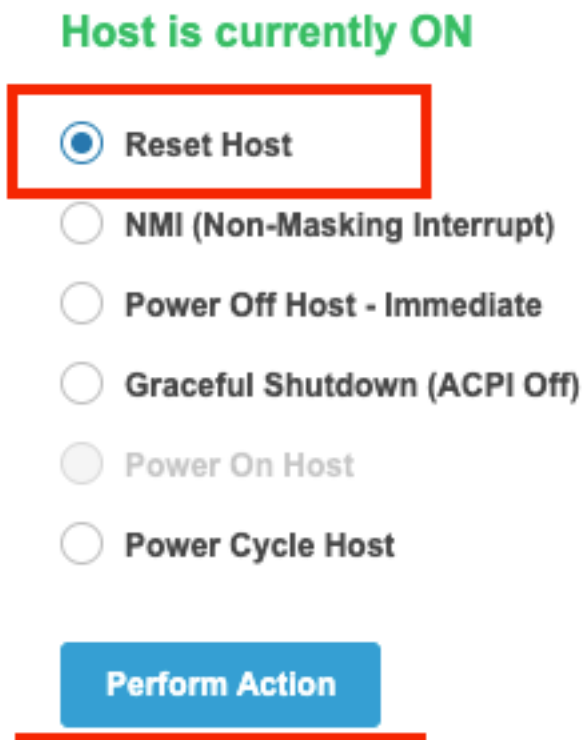


Fig. 18: Virtual Front Panel menu location

Fig. 19: Click **Perform Action** to reset the host

Warning: While the intrusion alarm is active the system fans run at a higher fixed speed than normal. Re-arming the intrusion sensor returns the fan to their typical profiled speeds.

2.4.1 Re-arm Using IPMI CLI Utilities

The intrusion switch can be re-armed using `ipmitool` either locally or over the network. The following steps assume the procedure is being performed locally on the **Netgate 8300**.

- Replace and fasten the chassis cover completely.
- Load the IPMI kernel module

```
# kldload ipmi
```

- Re-arm chassis intrusion sensor two times:

```
# ipmitool raw 0x04 0x2a 0x04 0x00
# ipmitool raw 0x04 0x2a 0x04 0x00
```

- Check the Chassis intrusion sensor, it should read a value of `0x0080`

```
# ipmitool sensor list | grep -i physical
Physical Scrtty | 0x0 | discrete | 0x0080 | na | na | na | na | na | na
```

- Unload the IPMI kernel module

```
# kldunload ipmi
```

2.5 Reinstalling pfSense Plus Software

This guide uses the [Netgate Installer](#) to install pfSense® Plus software on a **Netgate 8300** 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 the USB port on the left side of the front panel and boot the device.

The device will automatically attempt to boot from 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.

- On devices with a single NVMe drive, the only choice is `nda0`.
- On devices with multiple drives, such as MAX variants or those with manually added storage ([M.2 NVMe SSD Installation](#)), take care to choose the correct **ZFS Configuration** and intended target drive(s).

The most common use case for multiple drives in this device is a ZFS mirror, with both drives selected as targets.

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](#).

2.6 Configuring an OPT interface as an additional WAN

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 a **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 PriorityGateways 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

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

Configuring an additional LAN

- *Requirements*
- *Assign the Interface*
- *Interface Configuration*
- *DHCP Server*
- *Outbound NAT*
 - *Automatic or Hybrid Outbound NAT*
 - *Manual Outbound NAT*
- *Firewall Rules*
 - *Open*
 - *Isolated*
- *Other Services*

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  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  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  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:

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,

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Exceptions to Local Blocks											
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	OPTX subnets	*	This Firewall (self)	53 (DNS)	*	none	Allow clients to resolve DNS through the firewall	
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP any	OPTX subnets	*	This Firewall (self)	*	*	none	Allow client ICMP to the firewall	
Block to protected local networks											
<input type="checkbox"/>	✗	0/0 B	IPv4 *	*	*	This Firewall (self)	*	*	none	Reject all other traffic to the firewall	
<input type="checkbox"/>	✗	0/0 B	IPv4 *	*	*	PrivateNets	*	*	none	Reject all other traffic to private networks	
General pass rules											
<input type="checkbox"/>	✓	0/0 B	IPv4 *	OPTX subnets	*	*	*	*	none	Default allow all from OPTx	

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Fig. 20: Example firewall rules for isolated LAN type segment

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 8300. This button is located on the rear side of the unit toward the left end, between the power and console connectors and under the power button. See *Input and Output Ports* for reference photos.

See also:

- [Factory Reset from GUI or Console](#)

Unlike some other models of Netgate hardware, the reset procedure on Netgate 8300 can be triggered while the device is running and does not require complicated timing.

1. Power on the device if it is not already running.

If the device is booting, wait for the **Circle** LED to start flashing green or turn solid green.

2. **Press and hold** the reset button.

Note: This is the recessed button beneath the USB ports and may require a pen, paperclip, or similar tool to press.

The LEDs will start to fill in amber one by one (Circle, Square, then Diamond) while the button is held in the depressed state.

3. Continue holding in the button until **all** of the LEDs start flashing amber.

This will take approximately 8 seconds. Once the LEDs start flashing amber, the factory reset is in progress and the button can be released. The device will reboot automatically.

To cancel the reset procedure, release the button at any point *before* the LEDs begin to flash amber. The Circle LED will return to a solid green state indicating that the reset has been canceled.

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

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

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 Opening and Closing the Netgate 8300 Chassis

Some tasks may require opening up the chassis on the Netgate 8300 to access internal components. This document covers all steps required to open and close the chassis.

Opening and Closing the Netgate 8300 Chassis Outline

- *Warnings and Precautions*
- *Required Tools and Hardware*
- *Opening the Chassis*
 - *Power Off and Disconnect*
 - *Removing the Lid*
- *Closing the Chassis*
 - *Replacing and Fastening the Lid*
 - *Reconnect*
- *Re-arm the Intrusion Sensor*

2.9.1 Warnings and Precautions

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

Danger: Take all appropriate precautions and exercise care when handling the exposed system board and add-on cards. 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.**

Warning: This device includes an intrusion detection sensor which operates even when the device is without power.

Opening the case on this device triggers an intrusion alarm which is logged by the BMC and is visible in the IPMI sensors. **This alarm must be reset manually** as described in [Re-arm the Chassis Intrusion Switch](#).

When the intrusion alarm is active the fans run at a fixed speed of around 8500 RPM. Resetting the intrusion sensor alarm returns the fans to their profiled speed.

2.9.2 Required Tools and Hardware

Opening and closing the Netgate 8300 chassis requires the following tools and hardware:

- Phillips screwdriver
- Anti-static grounding strap and anti-static mat for handling the 8300 system

2.9.3 Opening the Chassis

Power Off and Disconnect

For safety, before opening the case, the Netgate 8300 must be **completely** disconnected. This includes power, network cables, USB cables, serial console cables, and any other external cables or devices connected to the Netgate 8300.

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 power off to the unit by changing the power switch on the rear of the unit to the **off** position.
2. Unplug the power cables from all installed power supply units (PSUs).

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

The LED indicator on all installed PSUs should be off before proceeding.

3. Unplug all network cables, USB cables and devices, serial console connections, etc.
4. Dismount the Netgate 8300 from the rack
5. Move the Netgate 8300 to a safe work location such as an anti-static mat



Fig. 21: Power switch (circled) in the off position

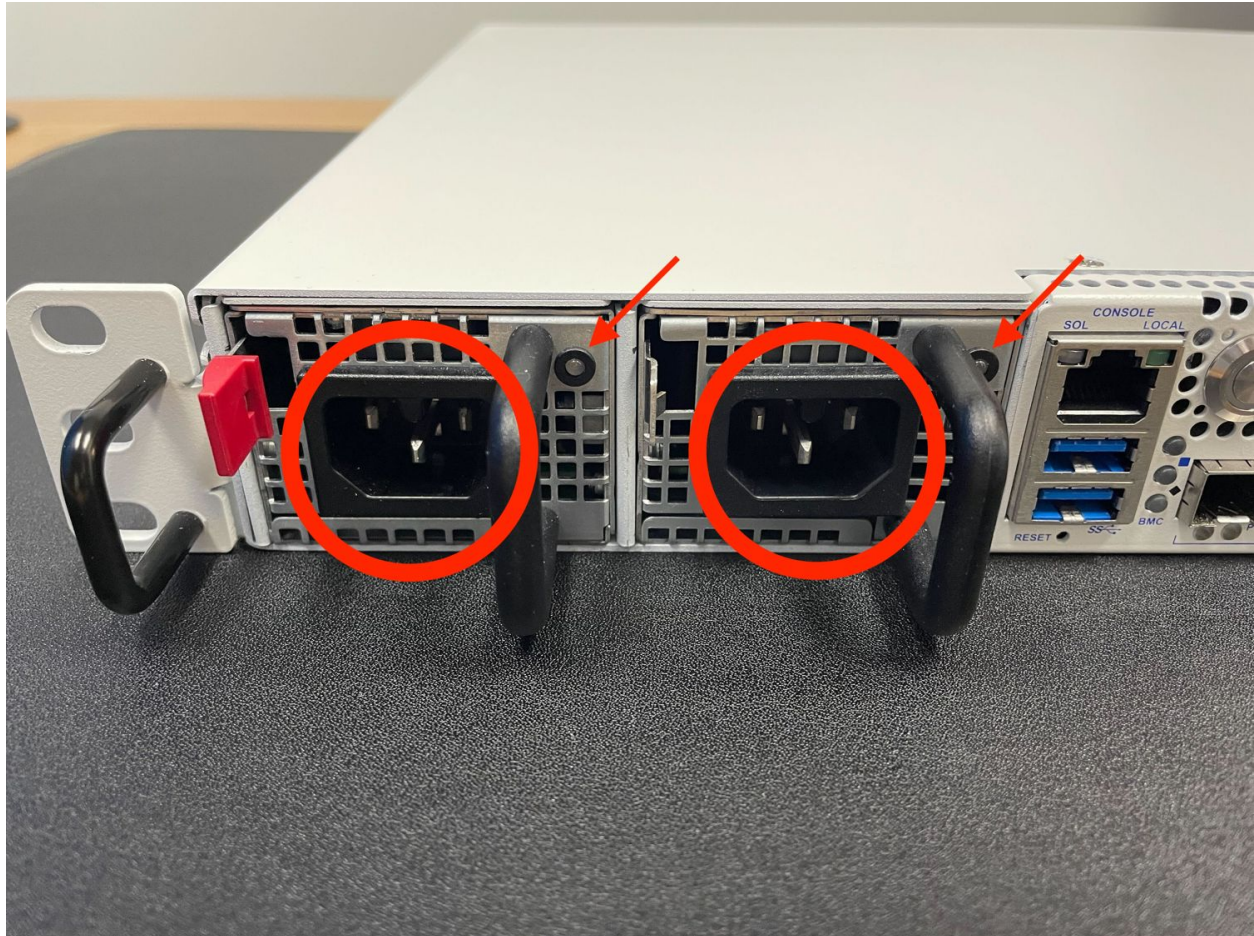


Fig. 22: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

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. Remove the screws from the top of the case near the front of the unit using the Phillips head screwdriver.

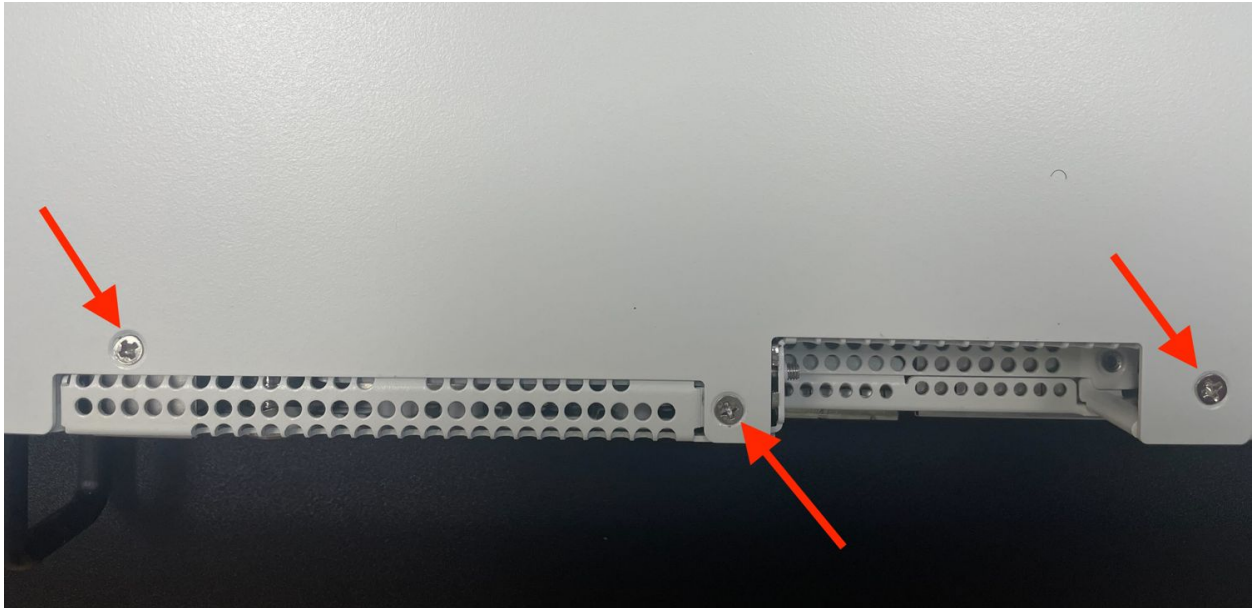


Fig. 23: Screws on the top of the cover at the front of the unit, indicated with arrows

2. Remove the screw from the rear side of the unit at the top left corner using the Phillips head screwdriver.
3. Remove the screw from the rear side of the unit at the top right corner using the Phillips head screwdriver.
4. Slide the top cover back away from the front panel until it stops.
5. Lift off the top cover and set it aside, keeping it upright to avoid damaging the top surface.

2.9.4 Closing the Chassis

Replacing and Fastening the Lid

With the internal components all in place, the next step is to replace the lid and all its 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 top cover with the top of the unit, a short distance behind the front panel.

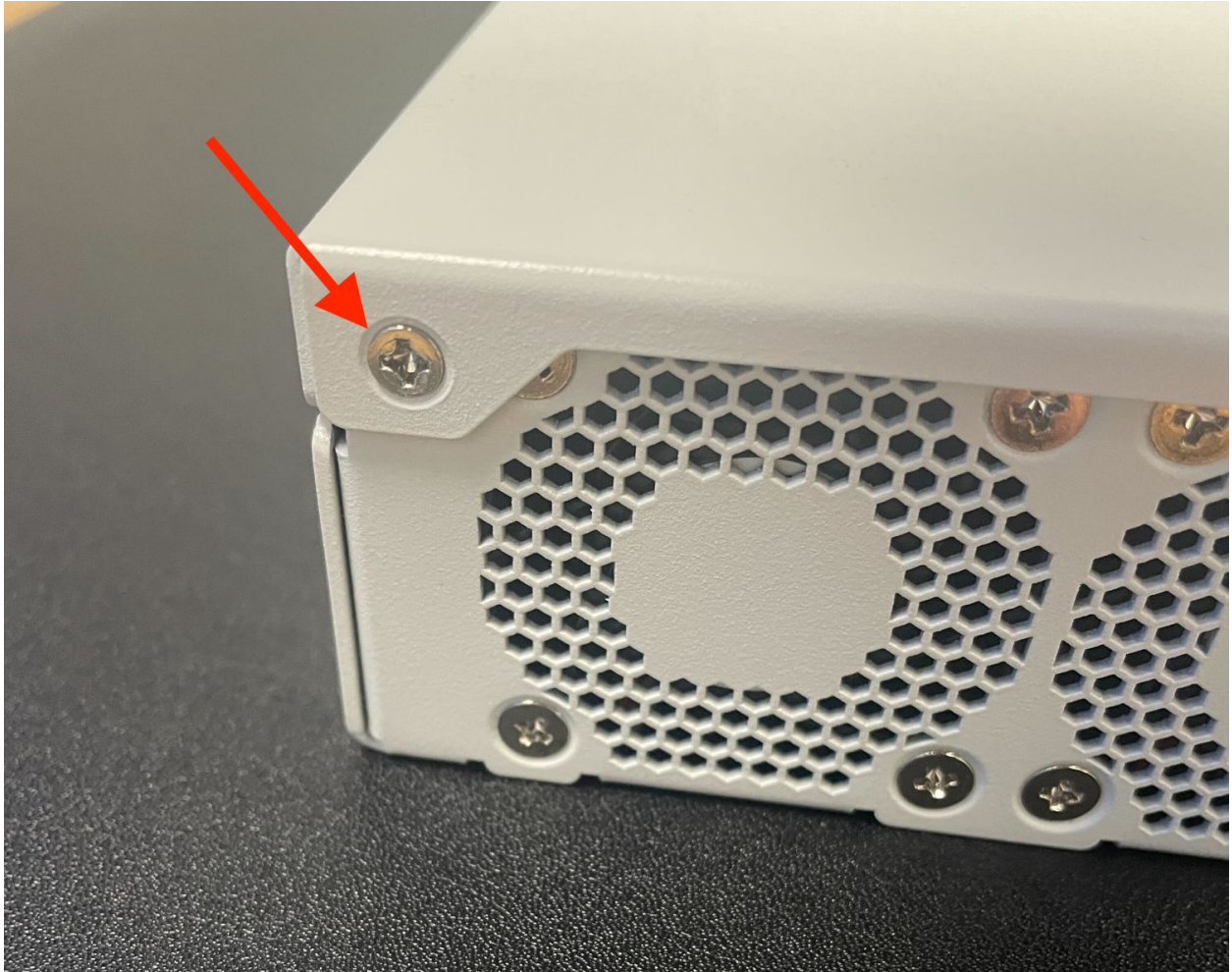


Fig. 24: Screw on the rear side of the unit at the left top corner, indicated with an arrow.



Fig. 25: Screw on the rear side of the unit at the right top corner, indicated with an arrow.



Fig. 26: Sliding back the top cover away from the front panel

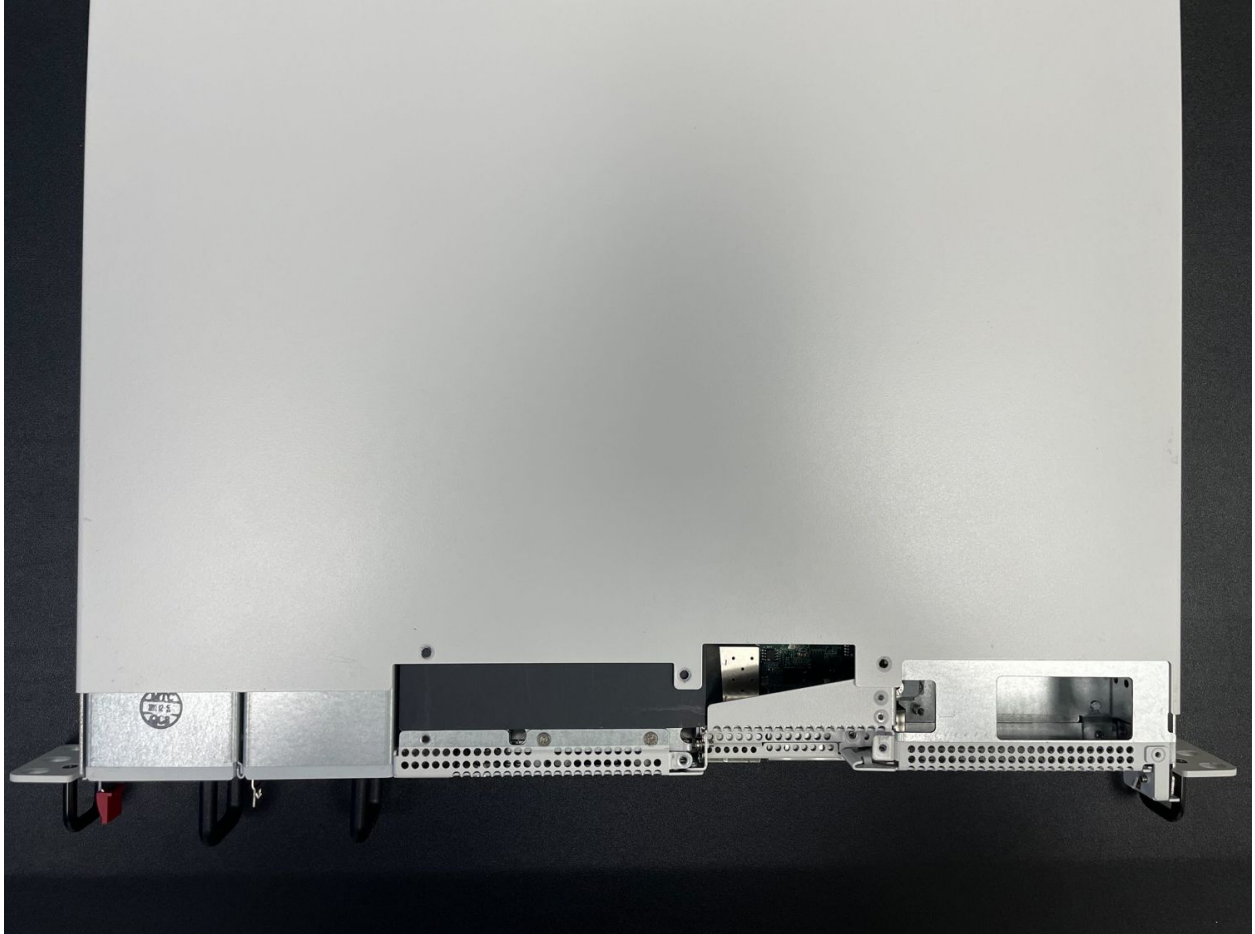


Fig. 27: Top cover in position to be lifted off

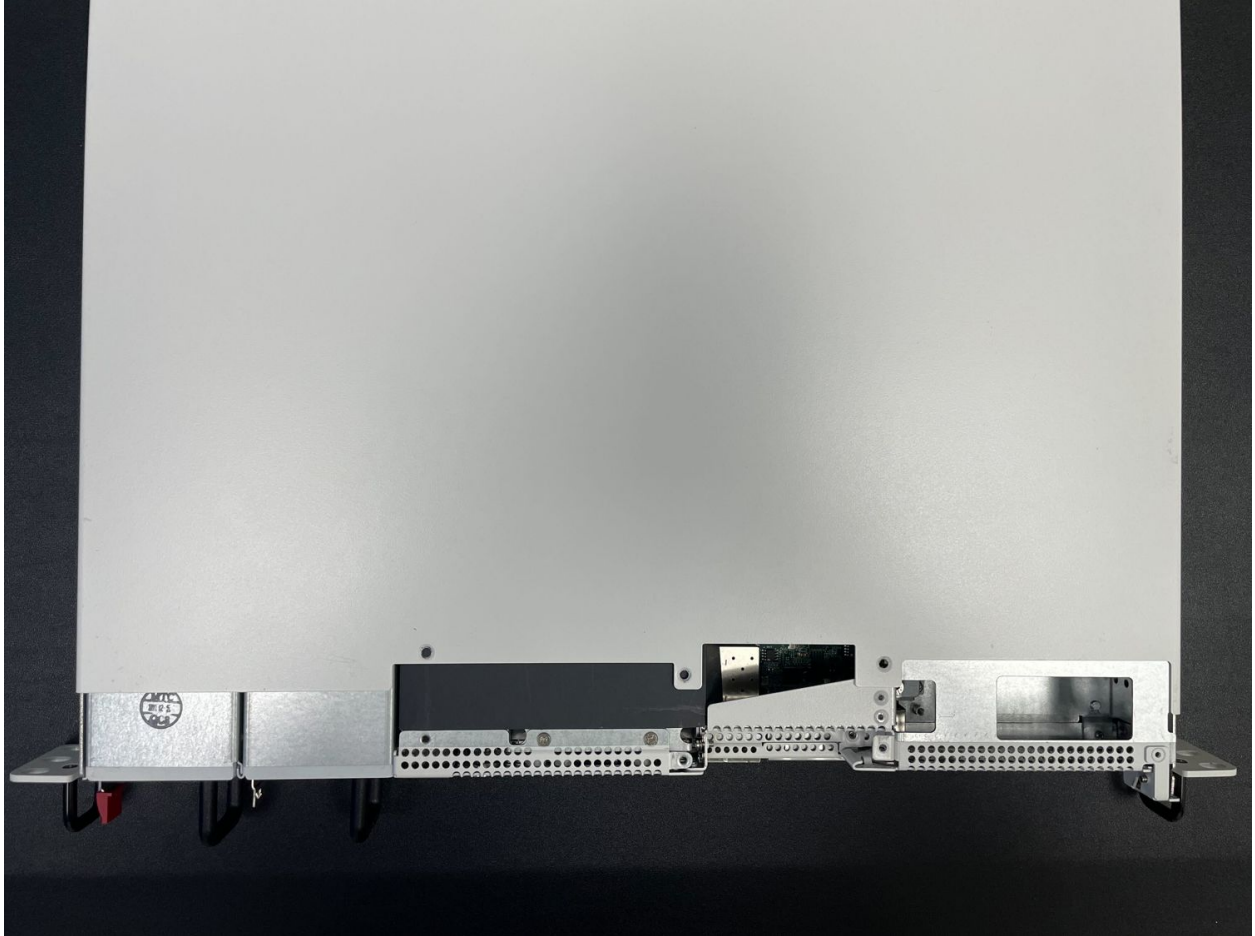


Fig. 28: Top cover in position to be replaced

2. Slide the top cover toward the front of the unit into its closed position.



Fig. 29: Slide the top cover back toward the front panel

Replace the screws on the rear of the unit (left and right top corners) using the Phillips head screwdriver.

Replace the screws on the top of the unit using the Phillips head screwdriver.

Reconnect

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

1. Mount the Netgate 8300 in the rack
2. Plug in all network cables, USB cables and devices, serial console connections, etc.
3. Insert the USB memstick containing the installation media
4. Plug the power cables into all installed power supply units.
5. Turn power on to the unit by changing the power switch on the rear of the unit to the **on** position.
6. Reconnect to the serial console

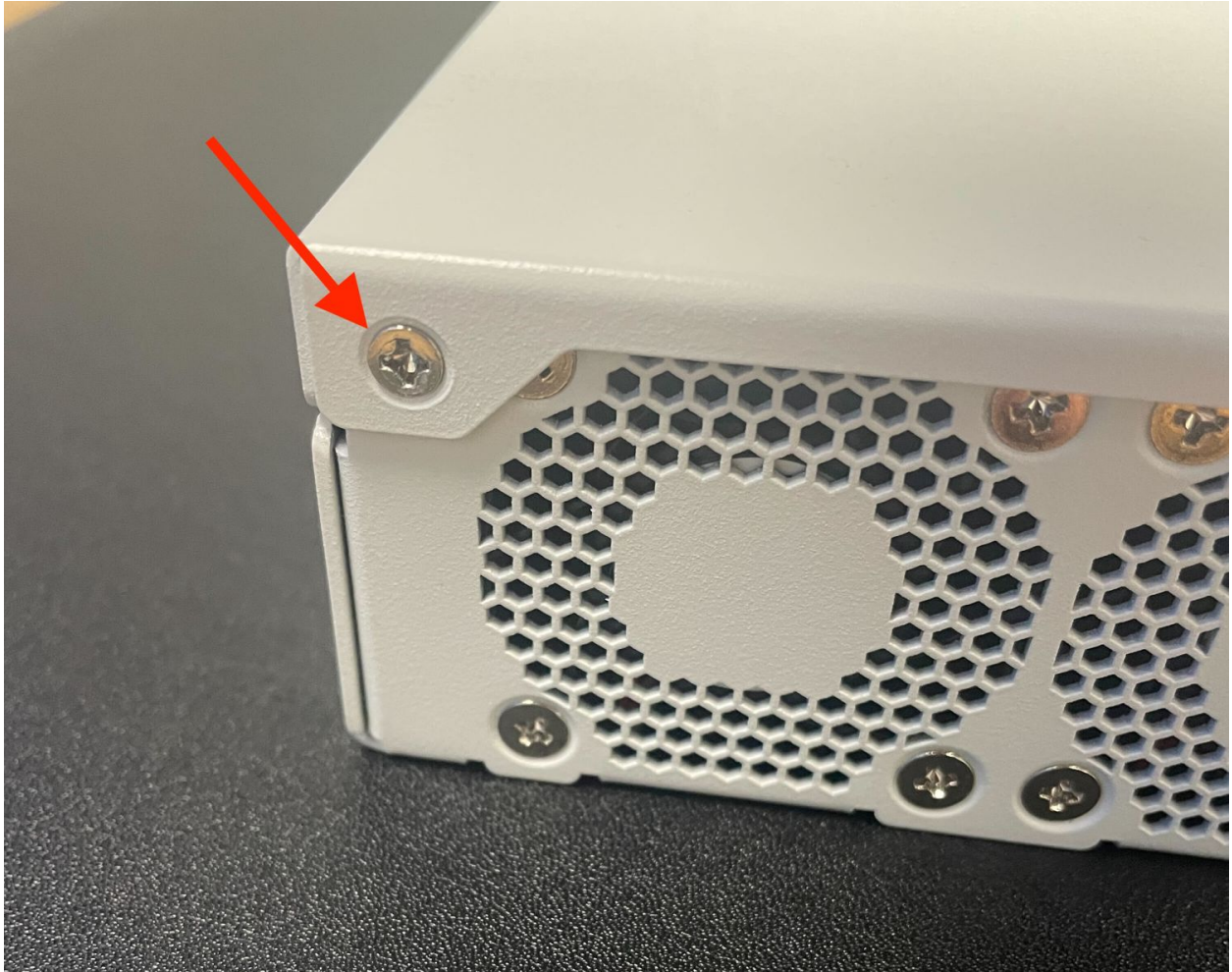


Fig. 30: Screw on the rear side of the unit at the left top corner, indicated with an arrow.



Fig. 31: Screw on the rear side of the unit at the right top corner, indicated with an arrow.

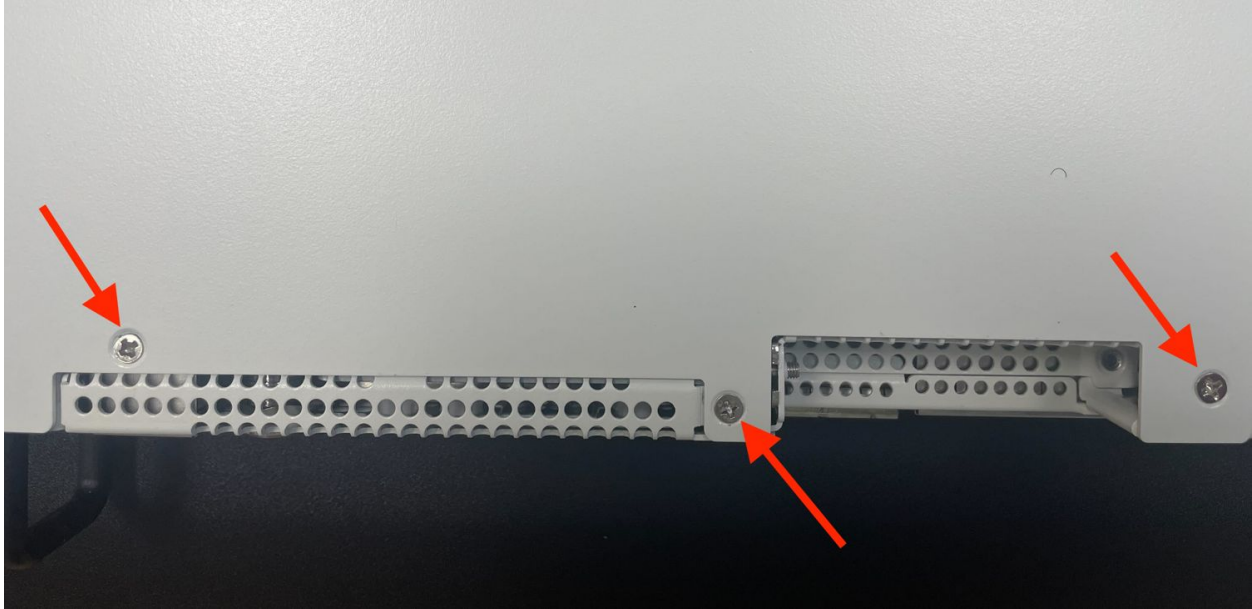


Fig. 32: Screws on the top of the cover at the front of the unit, indicated with arrows

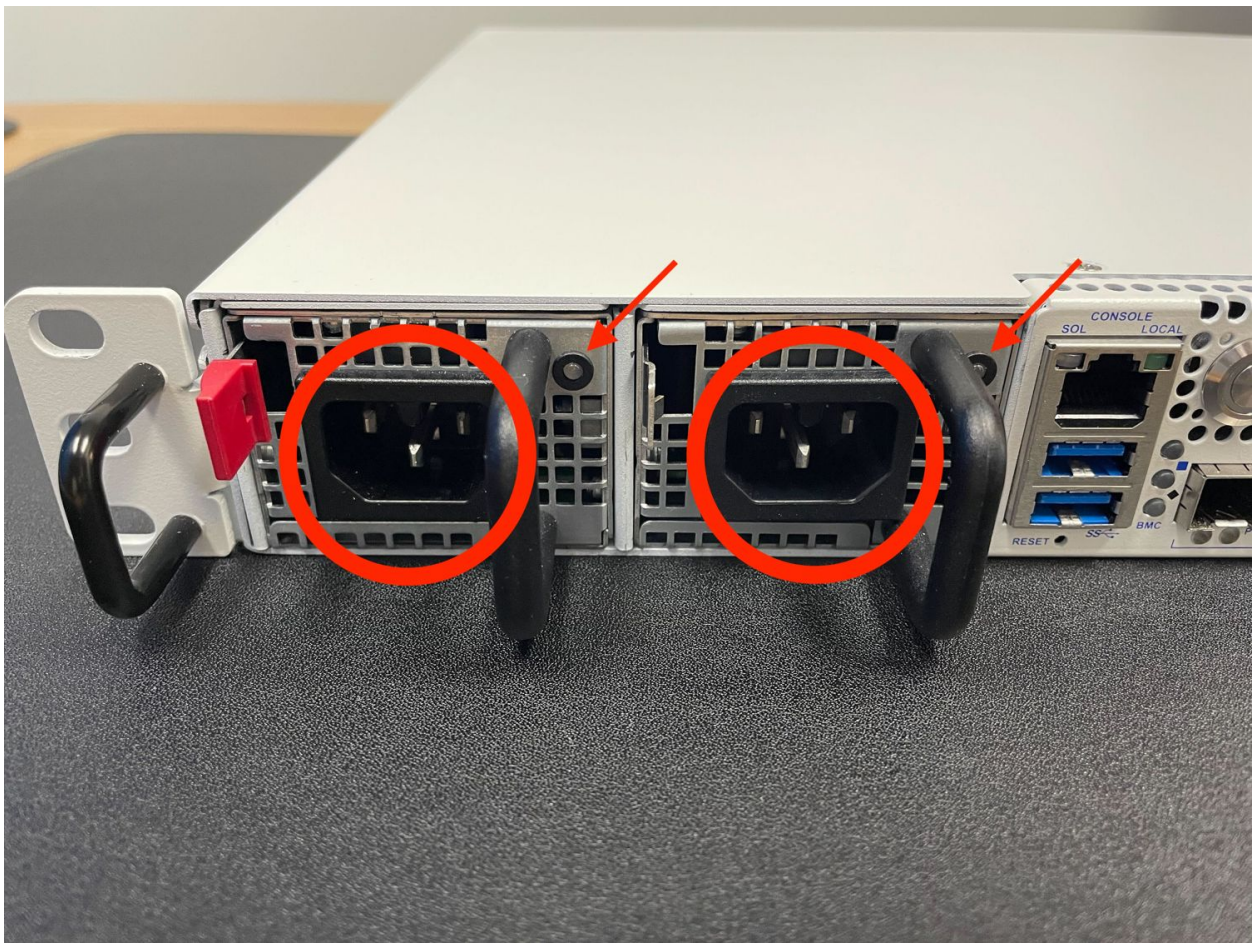


Fig. 33: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

2.9.5 Re-arm the Intrusion Sensor

Opening the case triggers the intrusion alarm sensor, even when the device is removed from power. The intrusion alarm causes the fans to run at a higher fixed speed until the sensor is re-armed.

Follow the procedure in *Re-arm the Chassis Intrusion Switch* to reset the sensor once the operating system is running.

2.10 M.2 NVMe SSD Installation

The Netgate® 8300 ships with one PCIe-based M.2 NVMe SSD. Optionally, a second PCIe-based M.2 NVMe drive can be installed as an upgrade.

Note: This guide assumes a second disk is being added for redundancy via ZFS mirroring.

M.2 NVMe SSD Installation Outline

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

2.10.1 Warnings and Precautions

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

Warning: pfSense® Plus software must be reinstalled using a ZFS mirror configuration to use a second M.2 NVMe SSD for redundancy.

Warning: The Netgate 8300 only supports PCIe-based M.2 NVMe storage devices. It **does not** support M.2 SATA devices.

Danger: Take all appropriate precautions and exercise care when handling the exposed system board and M.2 cards. 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.**

Warning: This device includes an intrusion detection sensor which operates even when the device is without power.

Opening the case on this device triggers an intrusion alarm which is logged by the BMC and is visible in the IPMI sensors. **This alarm must be reset manually** as described in *Re-arm the Chassis Intrusion Switch*.

When the intrusion alarm is active the fans run at a fixed speed of around 8500 RPM. Resetting the intrusion sensor alarm returns the fans to their profiled speed.

2.10.2 Required Tools and Hardware

Installing an M.2 NVMe SSD in the Netgate 8300 requires the following tools and hardware:

- Phillips screwdriver
- Anti-static grounding strap and anti-static mat for handling bare M.2 card and 8300 system
- 1 x PCIe-based M.2 NVMe SSD, 2280 or 2242 size, B+M-key or M-key card

See also:

The M.2 slot accepts both 2280 and 2242 size cards, but the device ships with the retaining clip set for a 2280 size card by default. This clip can easily be moved to accommodate a 2242 card without any tools.

2.10.3 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 installation, 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](#).

Power Off and Disconnect

For safety, before opening the case, the Netgate 8300 must be **completely** disconnected. This includes power, network cables, USB cables, serial console cables, and any other external cables or devices connected to the Netgate 8300.

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 power off to the unit by changing the power switch on the rear of the unit to the **off** position.



Fig. 34: Power switch (circled) in the off position

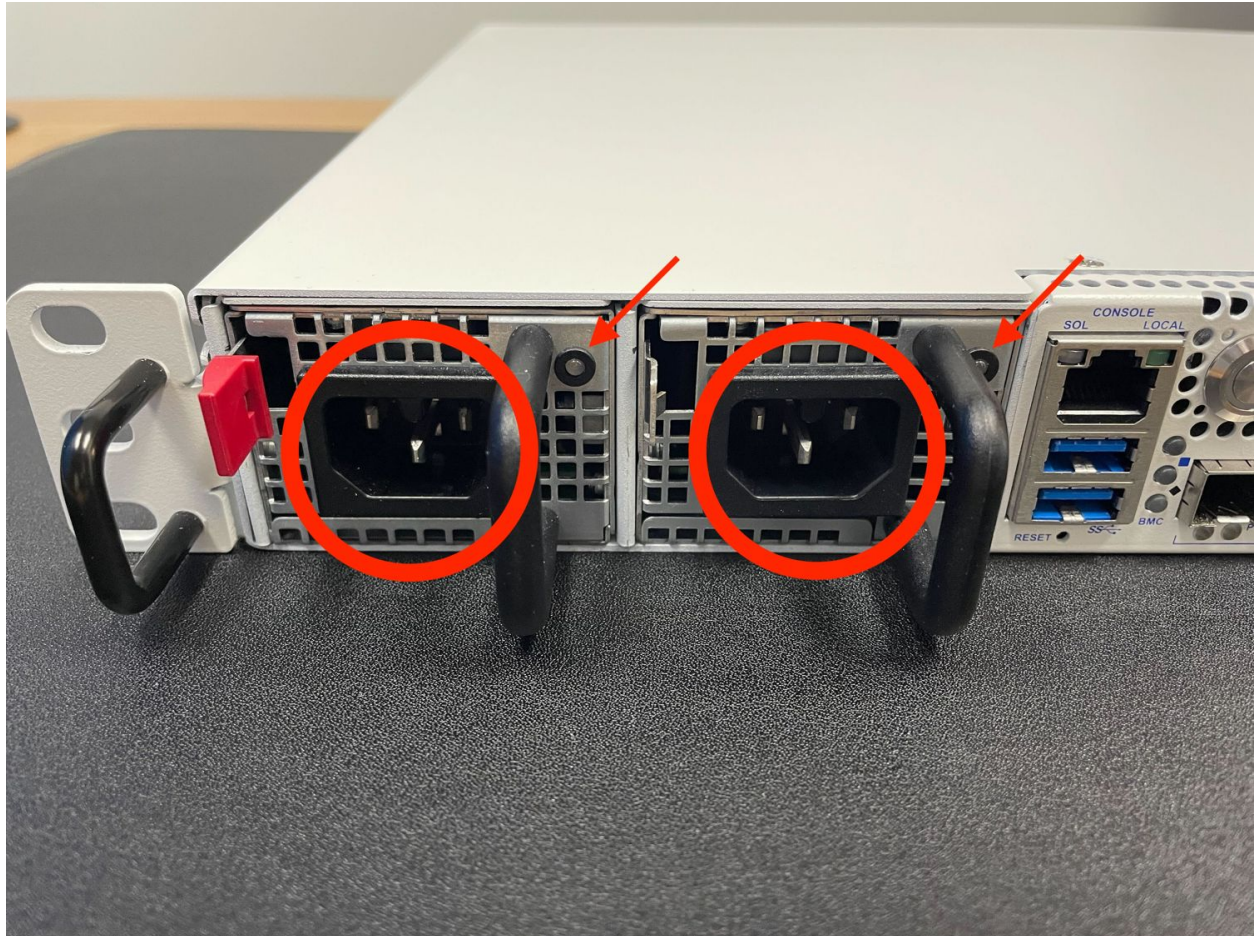


Fig. 35: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

2. Unplug the power cables from all installed power supply units (PSUs).

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

The LED indicator on all installed PSUs should be off before proceeding.

3. Unplug all network cables, USB cables and devices, serial console connections, etc.
4. Dismount the Netgate 8300 from the rack
5. Move the Netgate 8300 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. Remove the screws from the top of the case near the front of the unit using the Phillips head screwdriver.

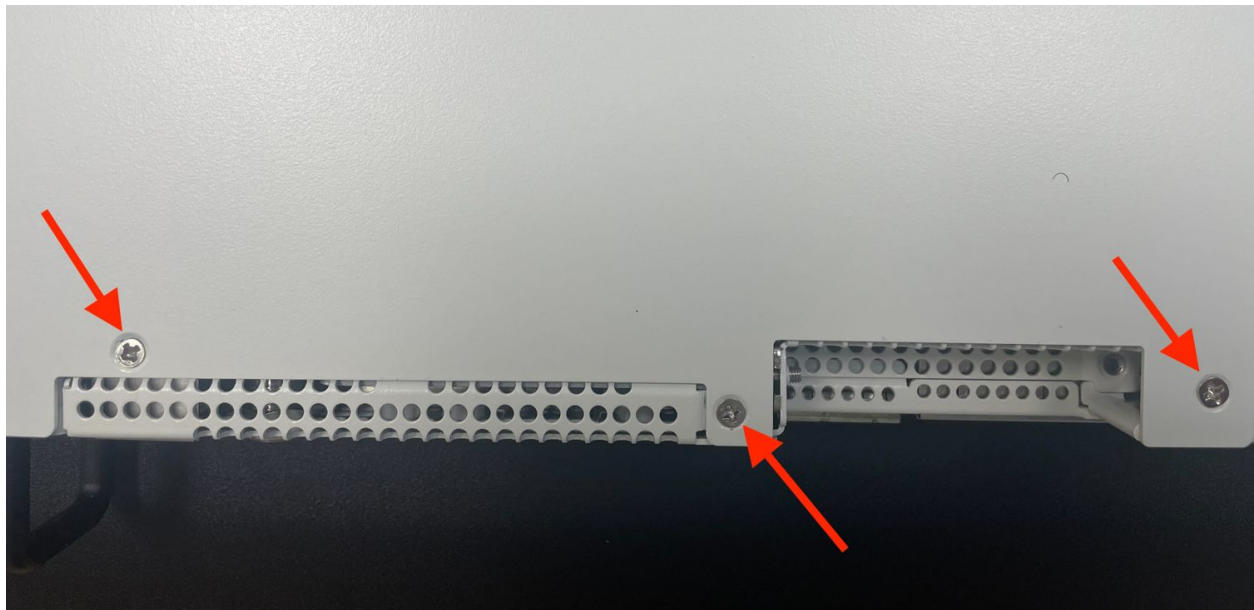


Fig. 36: Screws on the top of the cover at the front of the unit, indicated with arrows

2. Remove the screw from the rear side of the unit at the top left corner using the Phillips head screwdriver.
3. Remove the screw from the rear side of the unit at the top right corner using the Phillips head screwdriver.
4. Slide the top cover back away from the front panel until it stops.
5. Lift off the top cover and set it aside, keeping it upright to avoid damaging the top surface.



Fig. 37: Screw on the rear side of the unit at the left top corner, indicated with an arrow.



Fig. 38: Screw on the rear side of the unit at the right top corner, indicated with an arrow.



Fig. 39: Sliding back the top cover away from the front panel

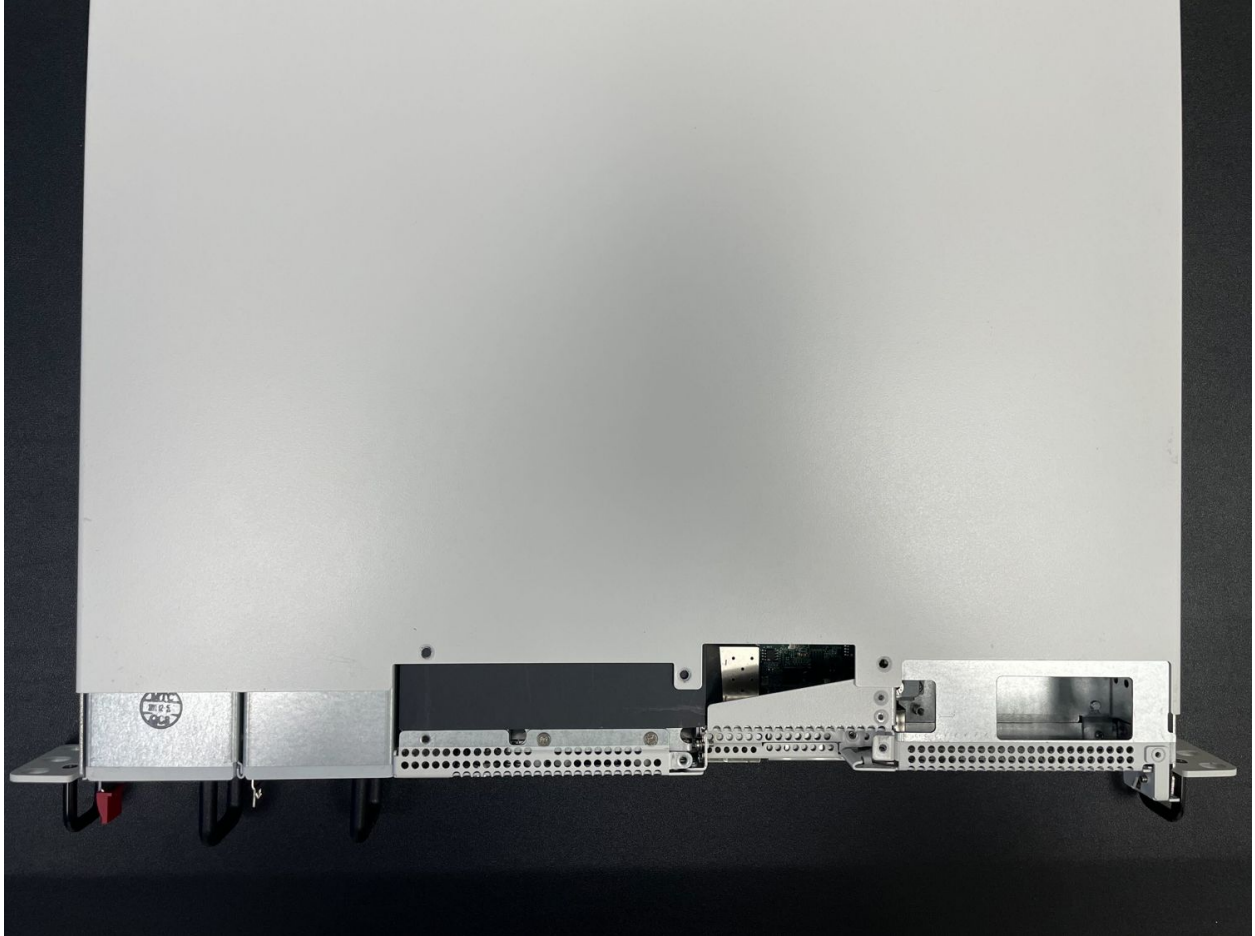


Fig. 40: Top cover in position to be lifted off

Move the Fan Duct

The M.2 NVMe riser card is located under the fan duct. This duct can be moved out of the way sufficiently enough to access the riser without completely removing it from the case.

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. Remove the screw retaining the side of the fan duct nearest to the PSU cages using the Phillips head screwdriver.

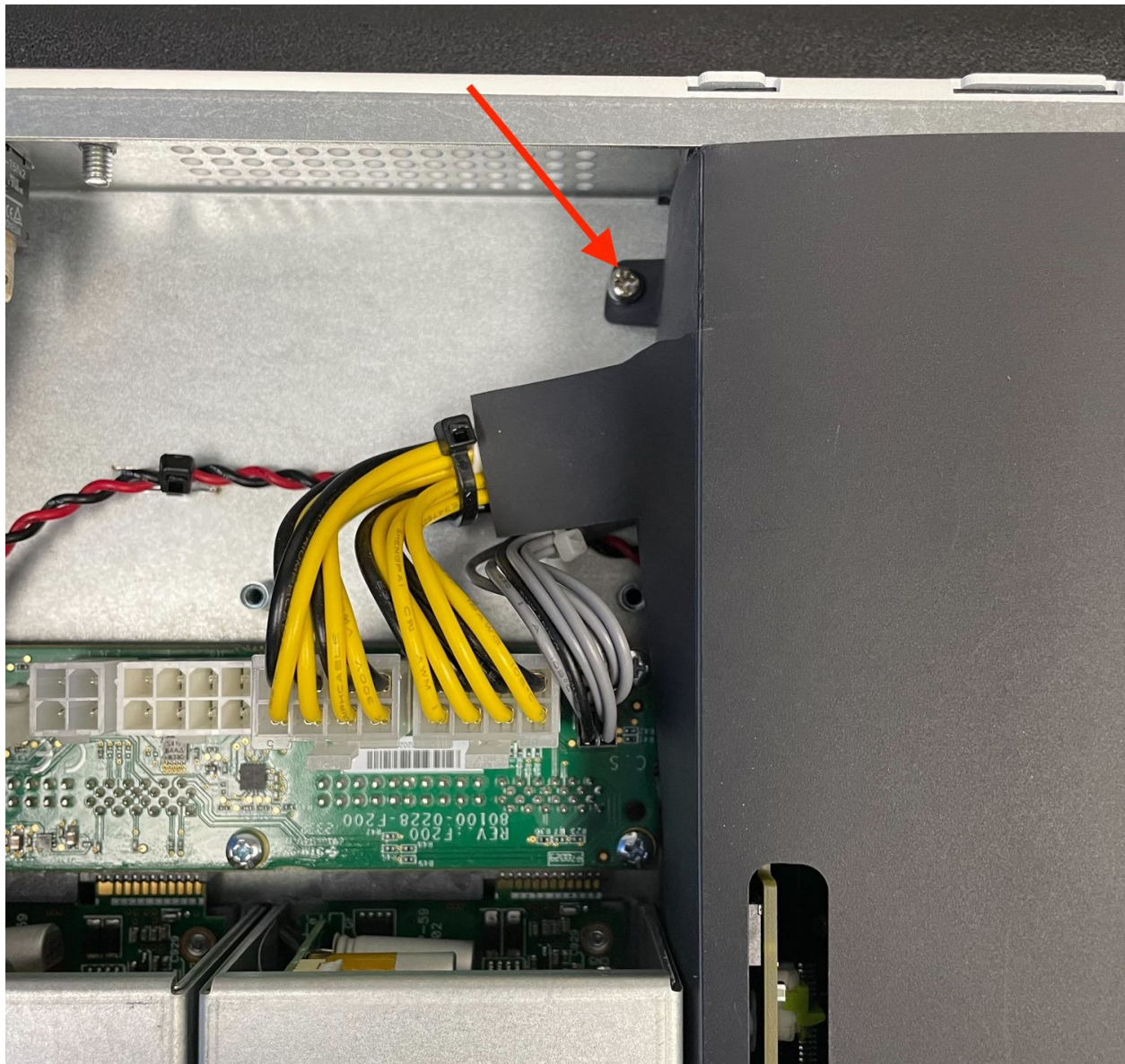


Fig. 41: Screw holding the fan duct in place, indicated with an arrow

2. Gently lift the side of the fan duct up and out of the way

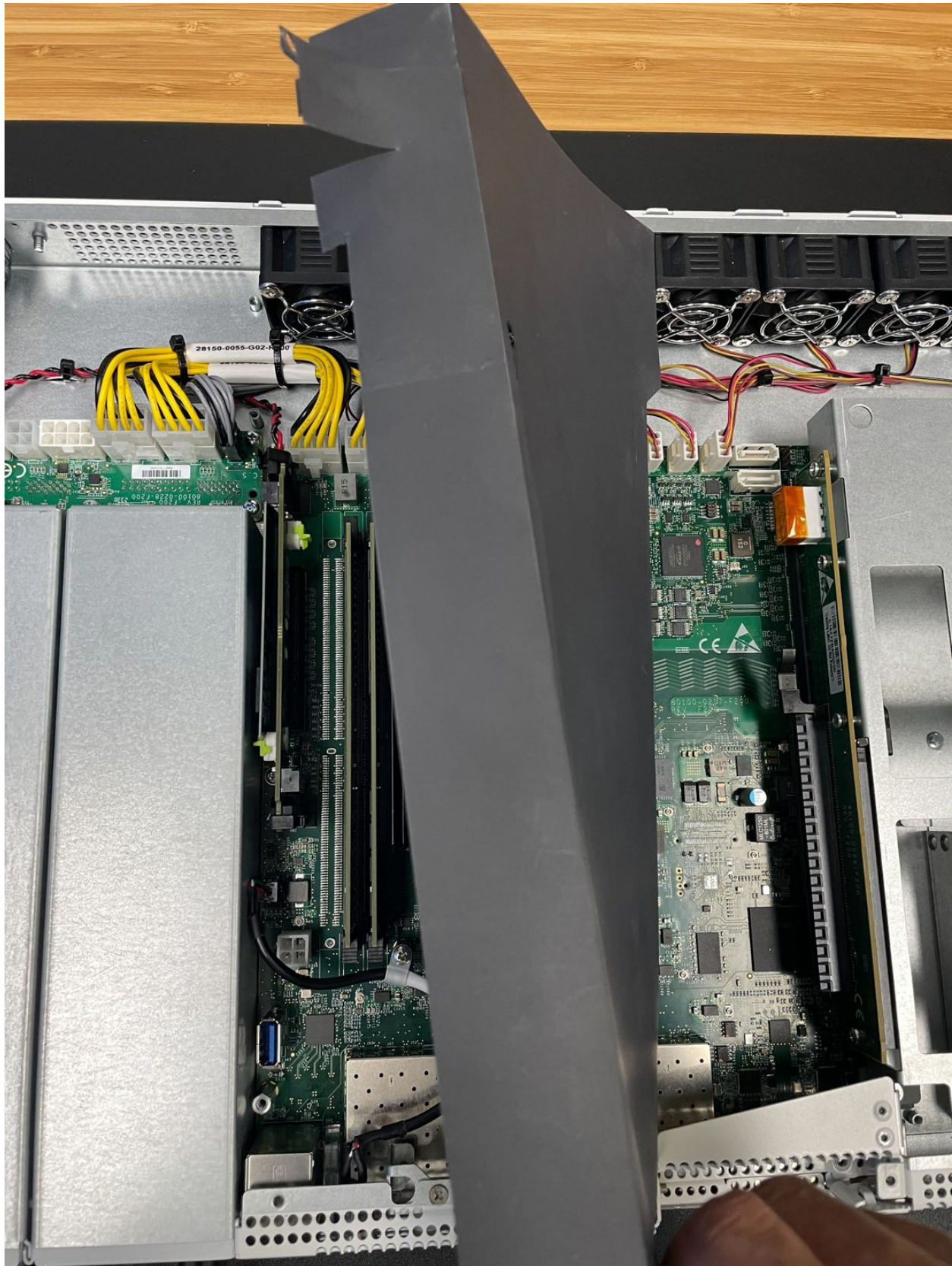


Fig. 42: Fan duct lifted out of the way to access the M.2 NVMe riser

Remove the M.2 NVMe Riser Card

The M.2 NVMe drives are located on a riser card near the PSU cages. This card must be removed to safely access the SSDs.

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 NVMe riser card

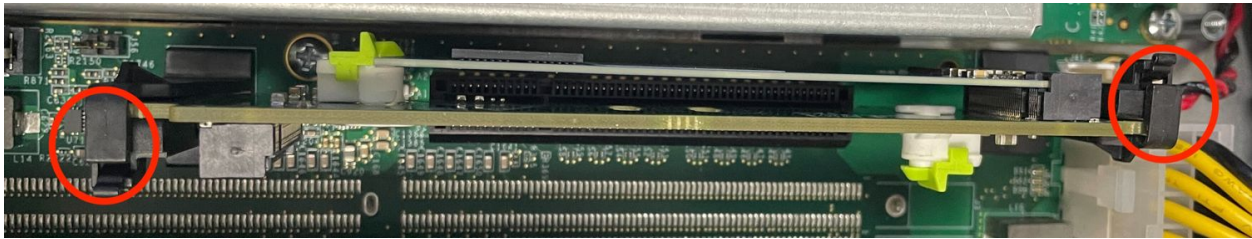


Fig. 43: M.2 NVMe riser card clips (circled) in the closed position

2. Lift both retaining clips holding the riser card in place to release the card

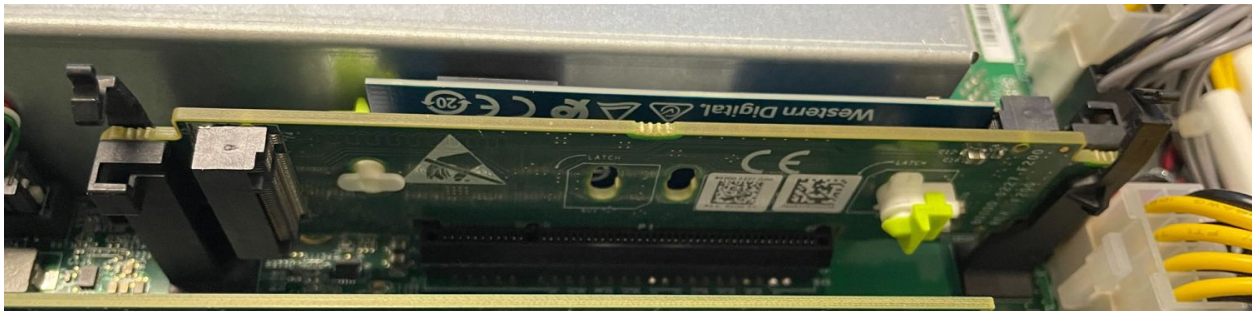


Fig. 44: M.2 NVMe riser card clips in the open position

3. Remove the riser card and set it aside

Install the SSD

With the riser card 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. Turn the riser card over so the second M.2 slot is visible.



Fig. 45: M.2 NVMe riser card slot 1 with the stock SSD installed

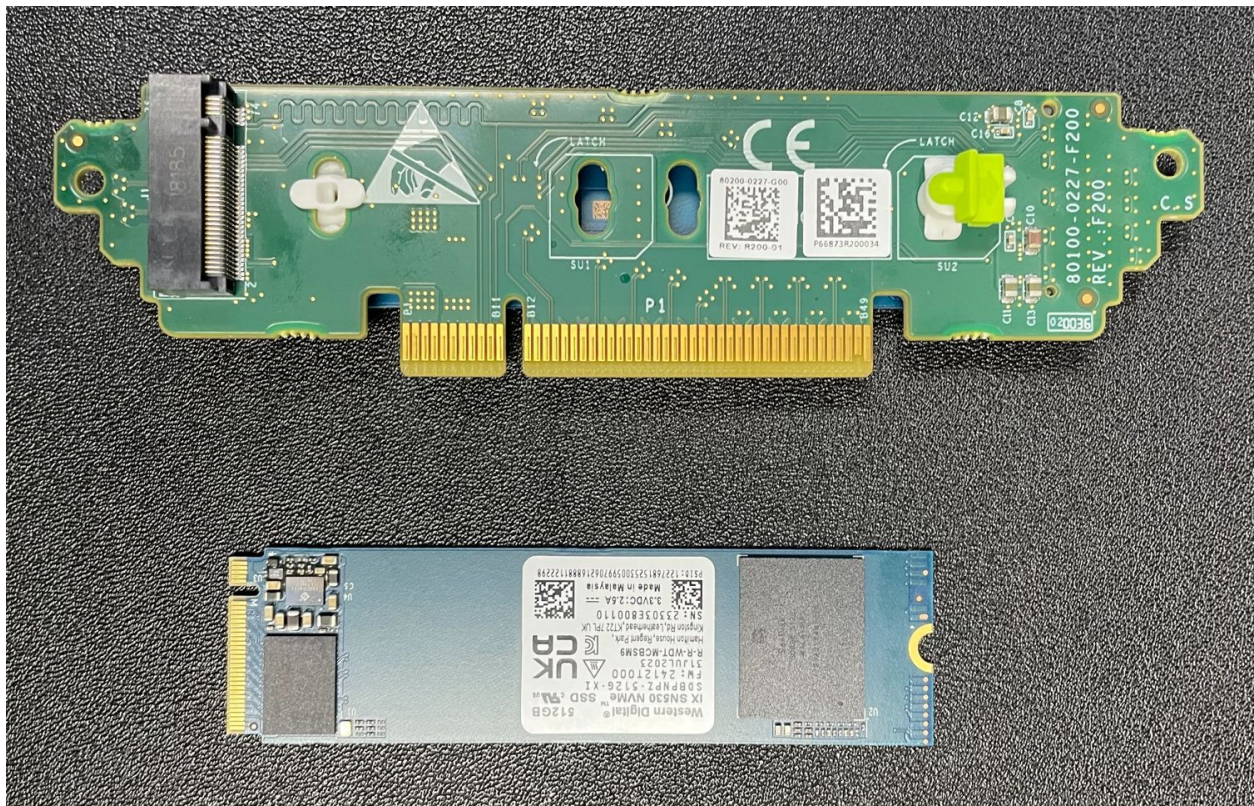


Fig. 46: M.2 NVMe riser card slot 2 (empty) and add-on M.2 NVMe SSD before install

Note: As mentioned earlier in this document, the Netgate 8300 currently supports M.2 B+M-Key or M-Key PCIe NVMe SSDs in 2280 or 2242 sizes.

2. Move the retainer clip to match the SSD size being installed.

The M.2 slot accepts both 2280 and 2242 size cards, but the device ships with the retaining clip set for a 2280 size card by default.

This clip can easily be moved to accommodate a 2242 card without any tools.

If the card being installed is a 2280 size card, these steps are unnecessary.

1. Rotate the retaining clip 90 degrees counterclockwise to release it.
 2. Lift the retaining clip away from the riser.
 3. Insert the retaining clip in the 2242 position hole outlined in white on the riser.
 4. Rotate the retaining clip 90 degrees clockwise to lock it in place.
3. Insert the M.2 card into the empty 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.

4. Gently push down the M.2 NMVe card until it snaps into place against the retaining clip.

There should be an audible “snap” sound as the retaining clip locks the drive into position.



Fig. 47: M.2 NVMe riser card slot 2 with the add-on SSD installed

Danger: Ensure that the retaining clip is fully engaged to avoid damaging the SSD!



Fig. 48: Close-up view of the M.2 retaining clip for slot 2 with the SSD secured

Replace the M.2 NVMe Riser Card and Fan Duct

With the new SSD installed, replace the riser card.

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. Insert the riser card back into its slot on the motherboard
2. Close the retaining clips to secure the riser card.
3. Move the fan duct back to its original location.
4. Secure the fan duct with its screw using the Phillips head screwdriver.

Replacing and Fastening the Lid

With the internal components all in place, the next step is to replace the lid and all its 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 top cover with the top of the unit, a short distance behind the front panel.
2. Slide the top cover toward the front of the unit into its closed position.

Replace the screws on the rear of the unit (left and right top corners) using
the Phillips head screwdriver.

Replace the screws on the top of the unit using the Phillips head screwdriver.

Reconnect

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

1. Mount the Netgate 8300 in the rack
2. Plug in all network cables, USB cables and devices, serial console connections, etc.
3. Insert the USB memstick containing the installation media
4. Plug the power cables into all installed power supply units.
5. Turn power on to the unit by changing the power switch on the rear of the unit to the **on** position.
6. Reconnect to the serial console



Fig. 49: Replacing the M.2 riser card

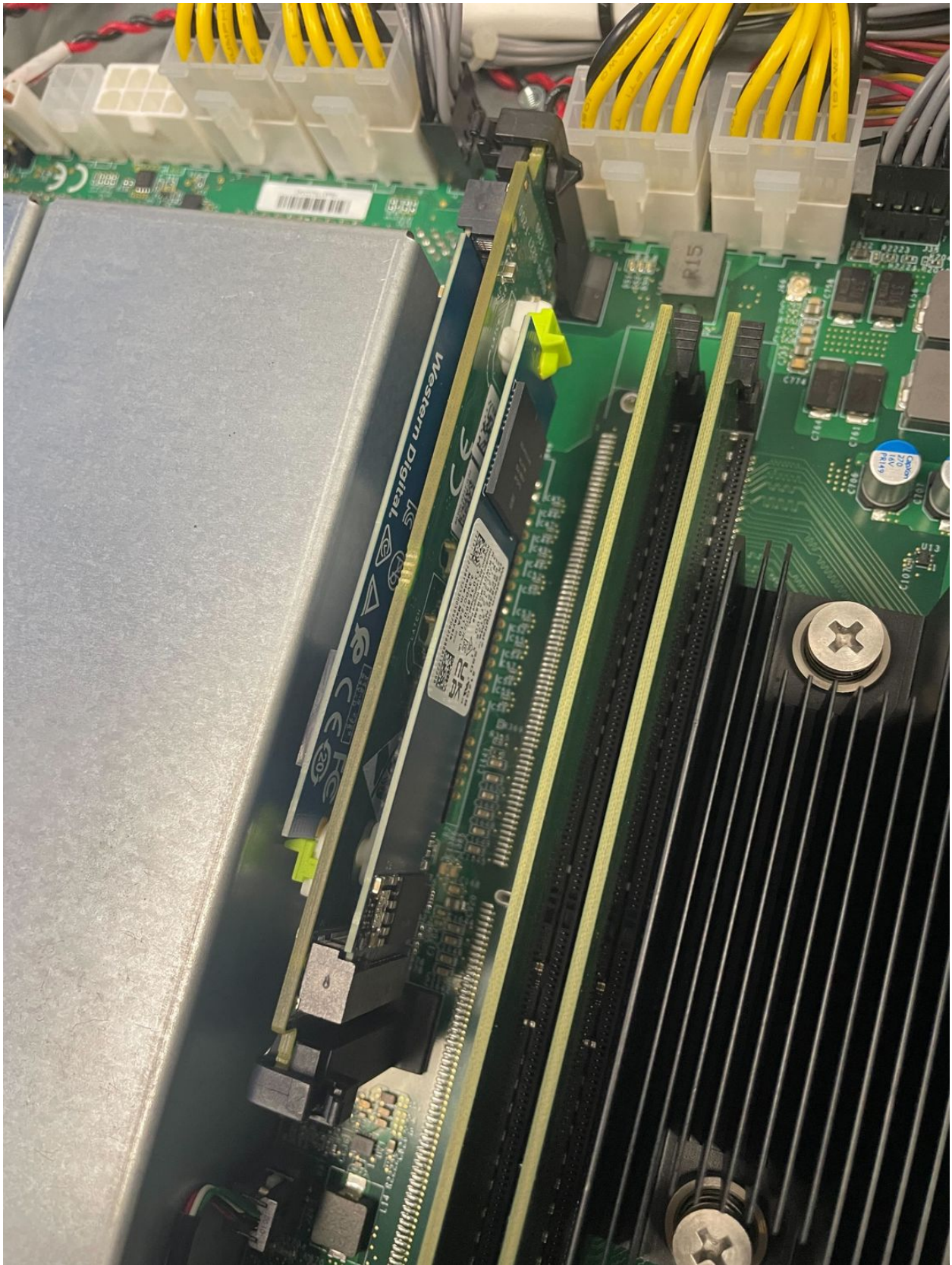


Fig. 50: M.2 riser card with two SSDs and riser clips in the closed position

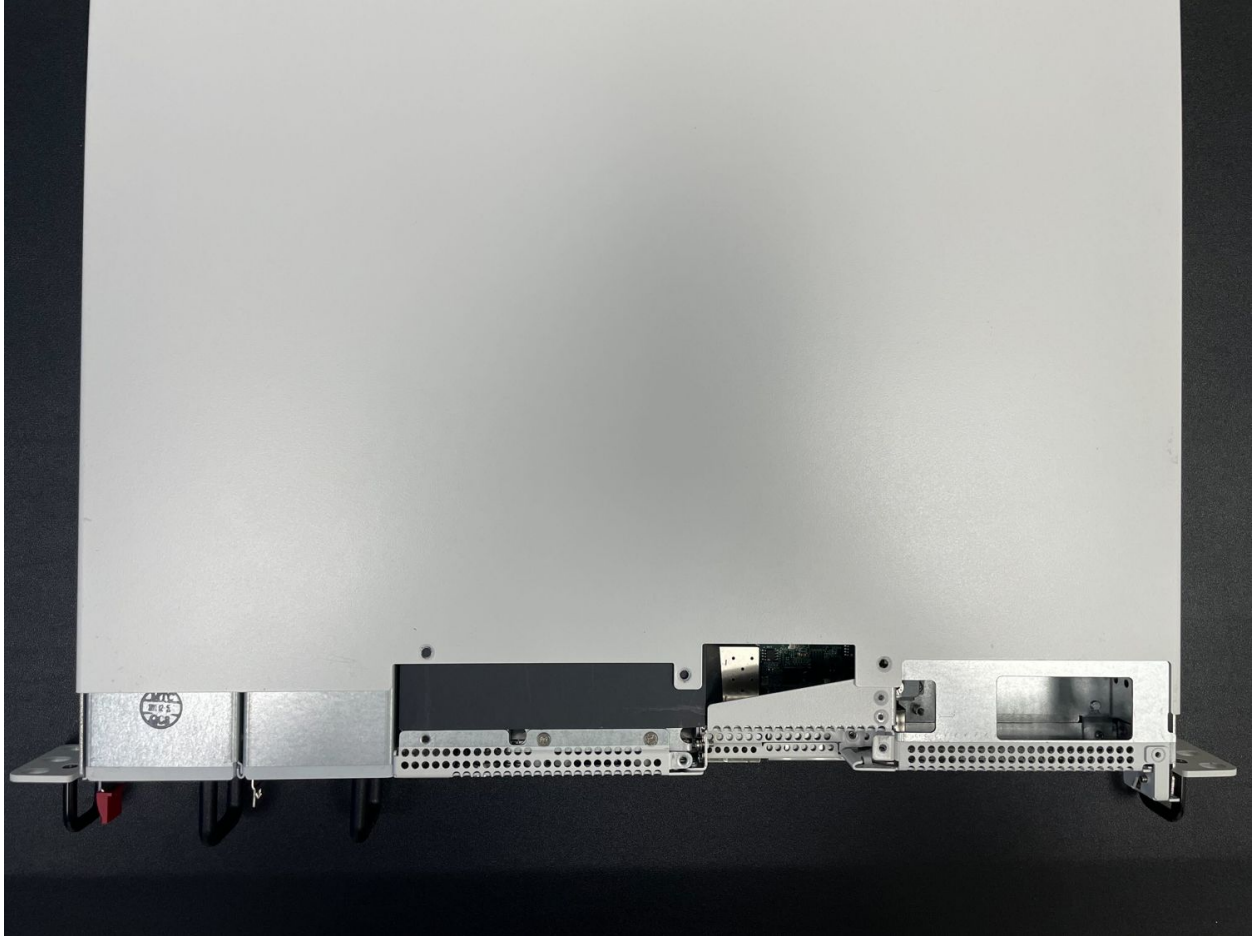


Fig. 51: Top cover in position to be replaced



Fig. 52: Slide the top cover back toward the front panel

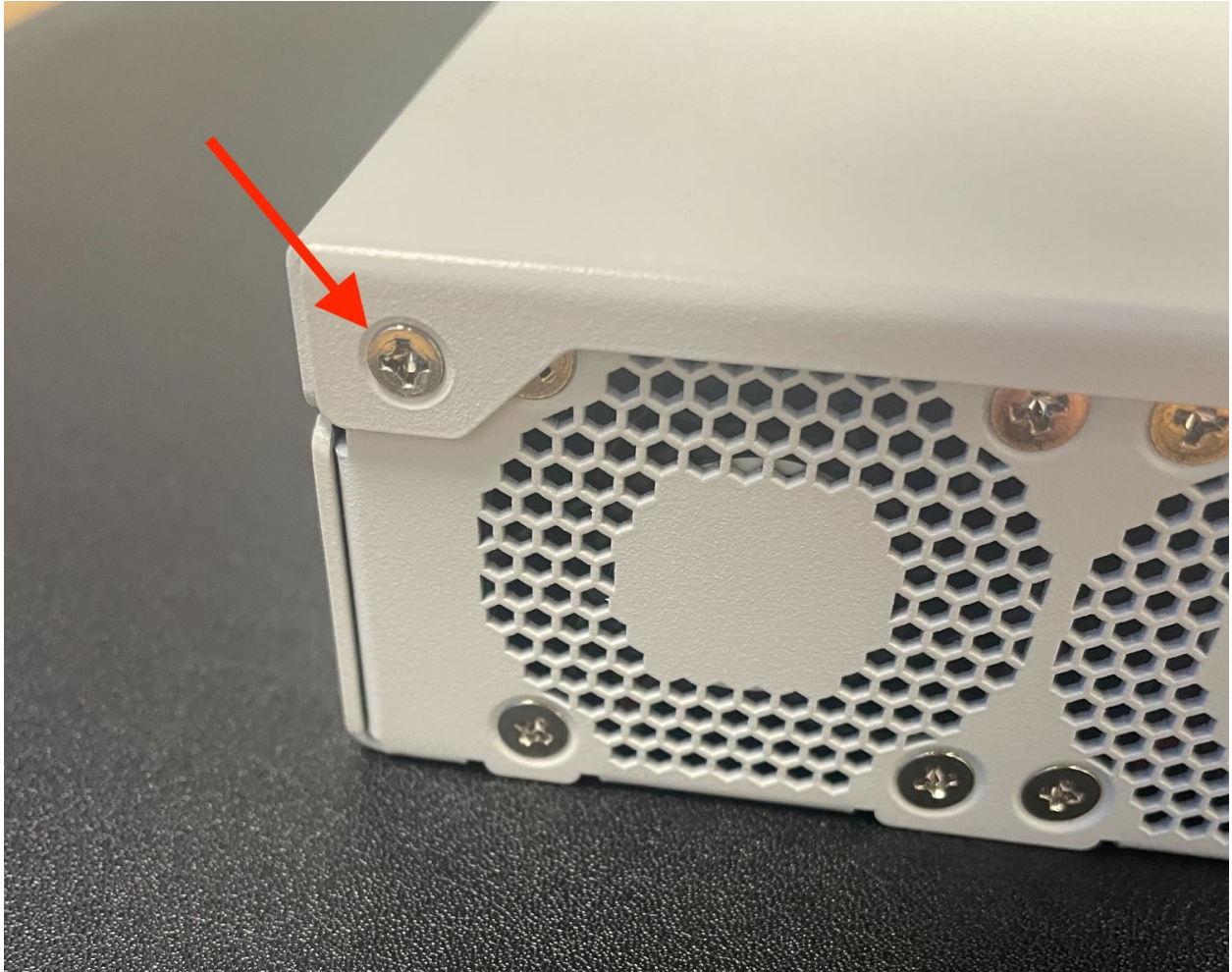


Fig. 53: Screw on the rear side of the unit at the left top corner, indicated with an arrow.



Fig. 54: Screw on the rear side of the unit at the right top corner, indicated with an arrow.

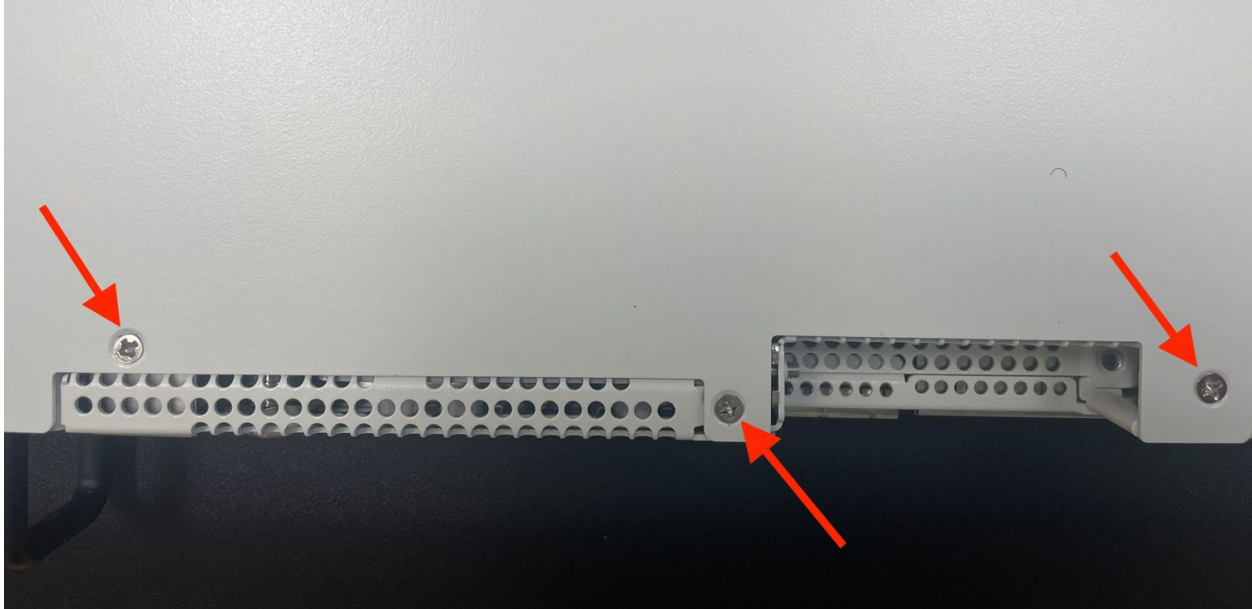


Fig. 55: Screws on the top of the cover at the front of the unit, indicated with arrows

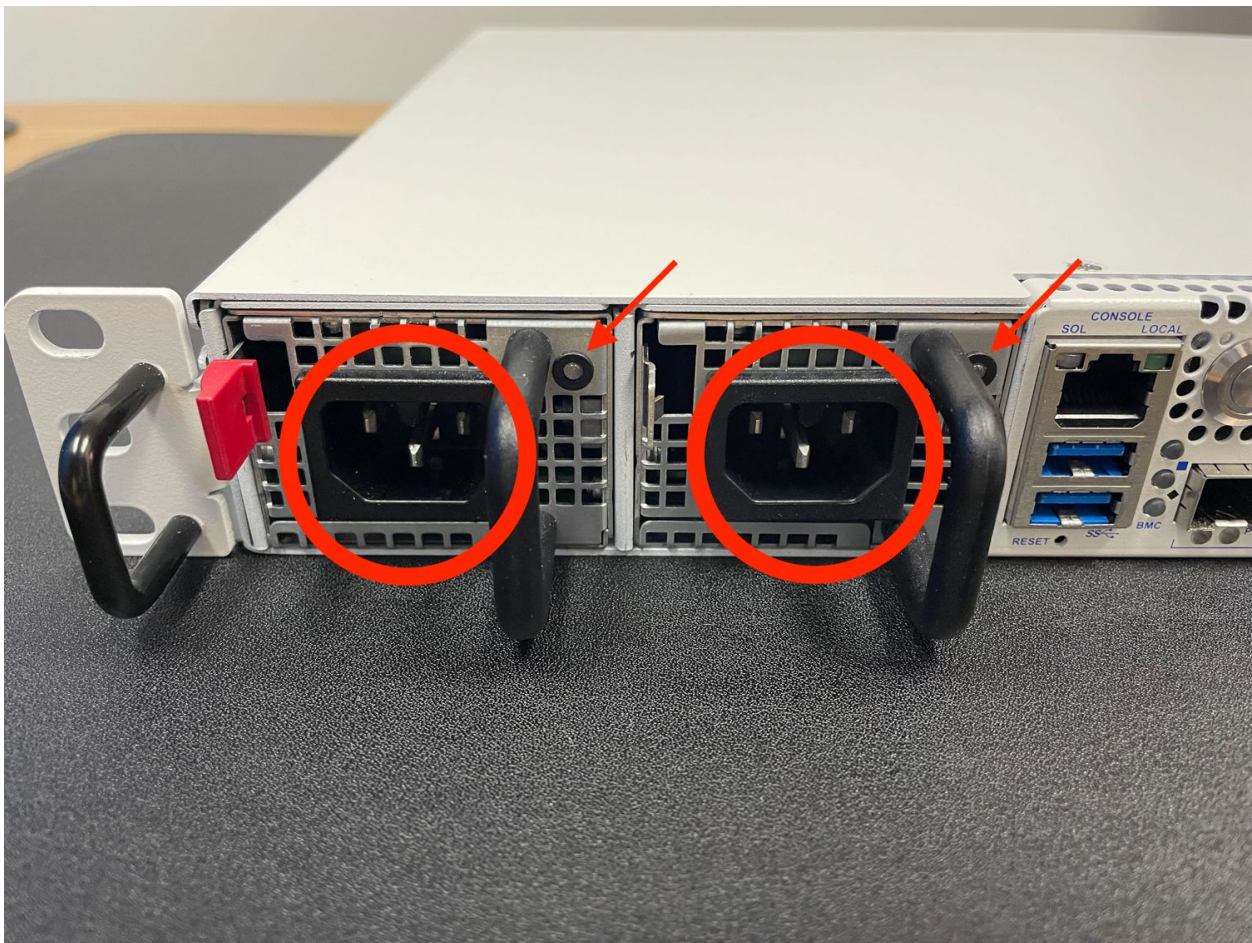


Fig. 56: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

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: When prompted to select a **ZFS Configuration** during the installation, choose **mirror**.

When prompted for drives, select **both** NVMe drives, which will be **nda0** and **nda1**.

The installer may select these drives automatically, but double check to be certain the selection is correct.

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

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](#).

Re-arm the Intrusion Sensor

Opening the case to install the new drive will have triggered the intrusion alarm sensor, even when the device was removed from power. The intrusion alarm causes the fans to run at a higher fixed speed until the sensor is re-armed.

Once pfSense software is up and running, follow the procedure in [Re-arm the Chassis Intrusion Switch](#) to reset the sensor.

2.11 Add-On Expansion Card Installation

The Netgate® 8300 has two expansion card slots available for additional devices such as 25 Gbit/s or 100 Gbit/s network interface cards.

The two expansion card slots have the following capabilities:

- 1x PCIe 3.0 x8 LP (Low Profile) slot which supports half-length low profile cards.
- 1x PCIe 4.0 x16 slot which supports full-height three-quarter length cards.

See also:

See [Input and Output Ports](#) for additional information on the expansion card slots.

Add-On Expansion Card Installation Outline

- [Warnings and Precautions](#)
- [Required Tools and Hardware](#)
- [Installation Procedure](#)

2.11.1 Warnings and Precautions

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

Warning: Installing network interface cards which use the same driver as built-in ports on the device will cause the existing interface assignments to shift, which will affect connectivity. Reinstalling or performing a factory reset will take expansion card(s) into account when the interfaces are automatically assigned.

See *Reassign Interfaces (Network Interface Cards Only)* later in this document for details.

Danger: Take all appropriate precautions and exercise care when handling the exposed system board and add-on cards. 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.**

Warning: This device includes an intrusion detection sensor which operates even when the device is without power.

Opening the case on this device triggers an intrusion alarm which is logged by the BMC and is visible in the IPMI sensors. **This alarm must be reset manually** as described in *Re-arm the Chassis Intrusion Switch*.

When the intrusion alarm is active the fans run at a fixed speed of around 8500 RPM. Resetting the intrusion sensor alarm returns the fans to their profiled speed.

2.11.2 Required Tools and Hardware

Installing add-on expansion cards in the Netgate 8300 requires the following tools and hardware:

- Phillips screwdriver
- Anti-static grounding strap and anti-static mat for handling bare components and the 8300 system
- Compatible expansion card

2.11.3 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, then the first step is to take a backup of that configuration for safety.

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](#).

Power Off and Disconnect

For safety, before opening the case, the Netgate 8300 must be **completely** disconnected. This includes power, network cables, USB cables, serial console cables, and any other external cables or devices connected to the Netgate 8300.

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 power off to the unit by changing the power switch on the rear of the unit to the **off** position.
2. Unplug the power cables from all installed power supply units (PSUs).

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

The LED indicator on all installed PSUs should be off before proceeding.

3. Unplug all network cables, USB cables and devices, serial console connections, etc.
4. Dismount the Netgate 8300 from the rack
5. Move the Netgate 8300 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. Remove the screws from the top of the case near the front of the unit using the Phillips head screwdriver.
2. Remove the screw from the rear side of the unit at the top left corner using the Phillips head screwdriver.



Fig. 57: Power switch (circled) in the off position

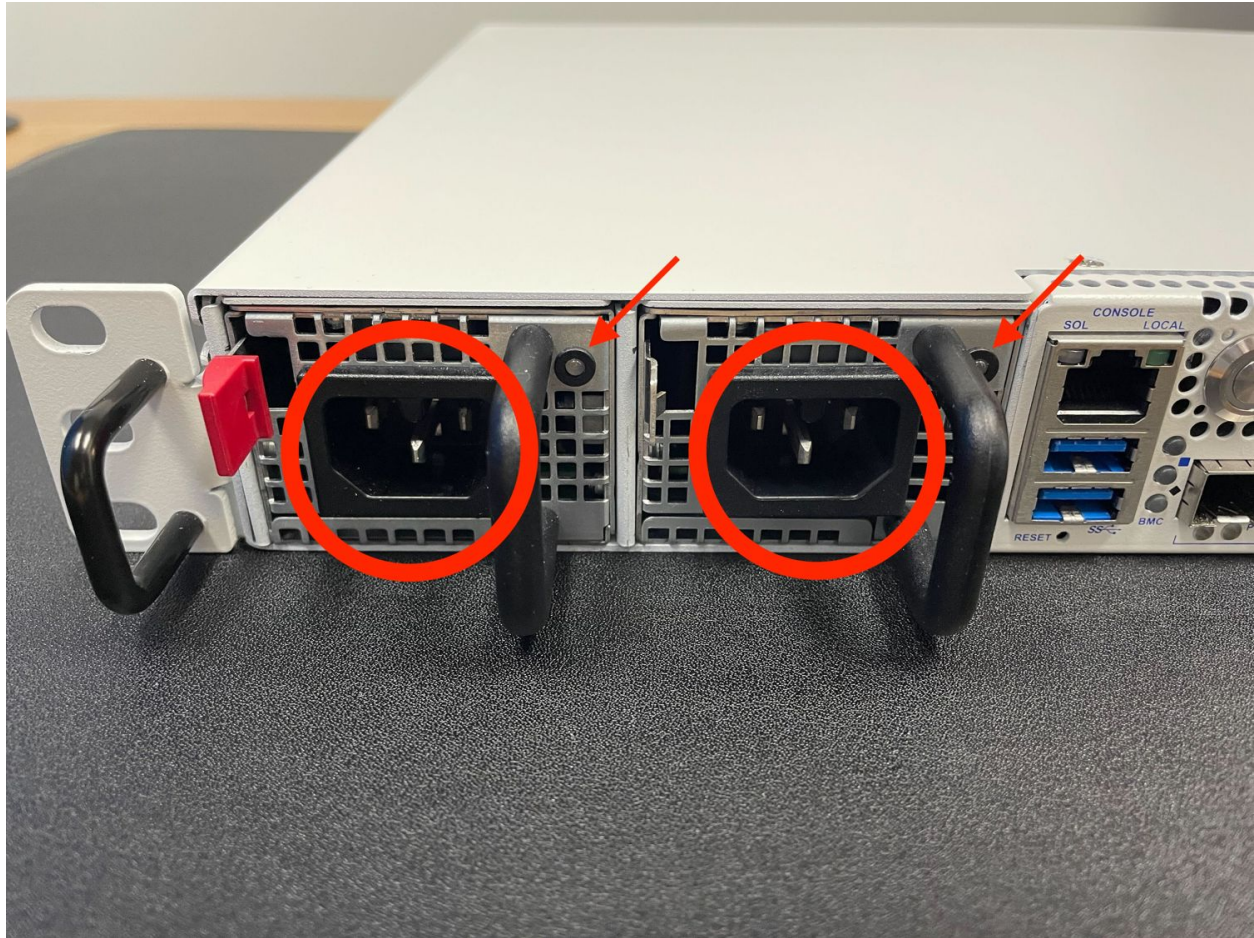


Fig. 58: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

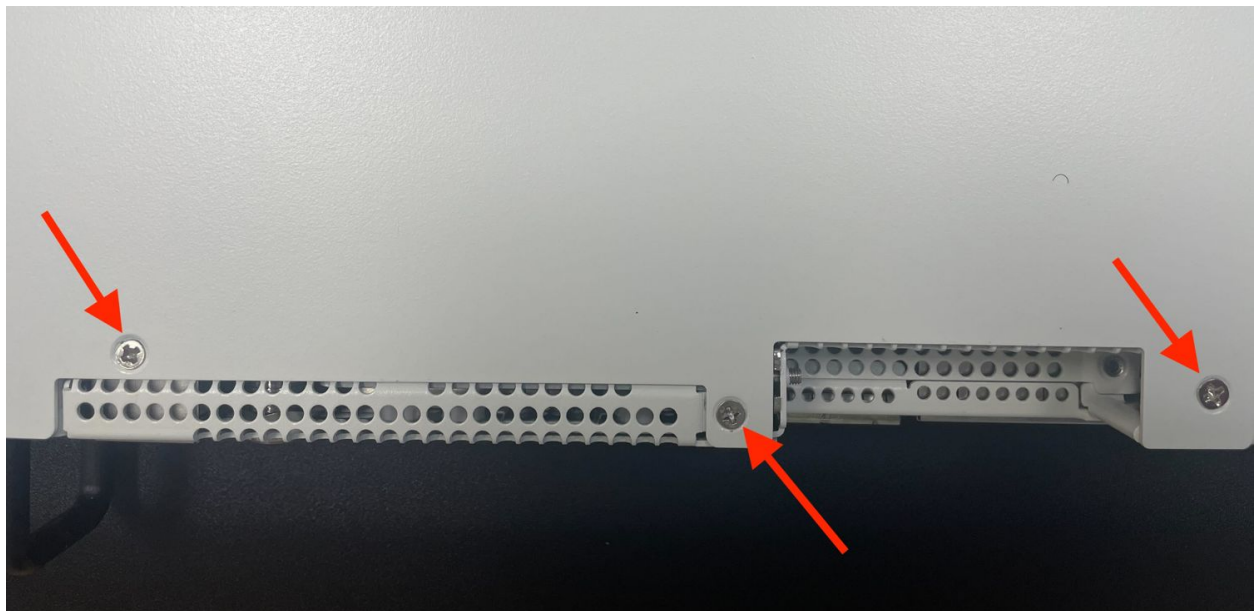


Fig. 59: Screws on the top of the cover at the front of the unit, indicated with arrows

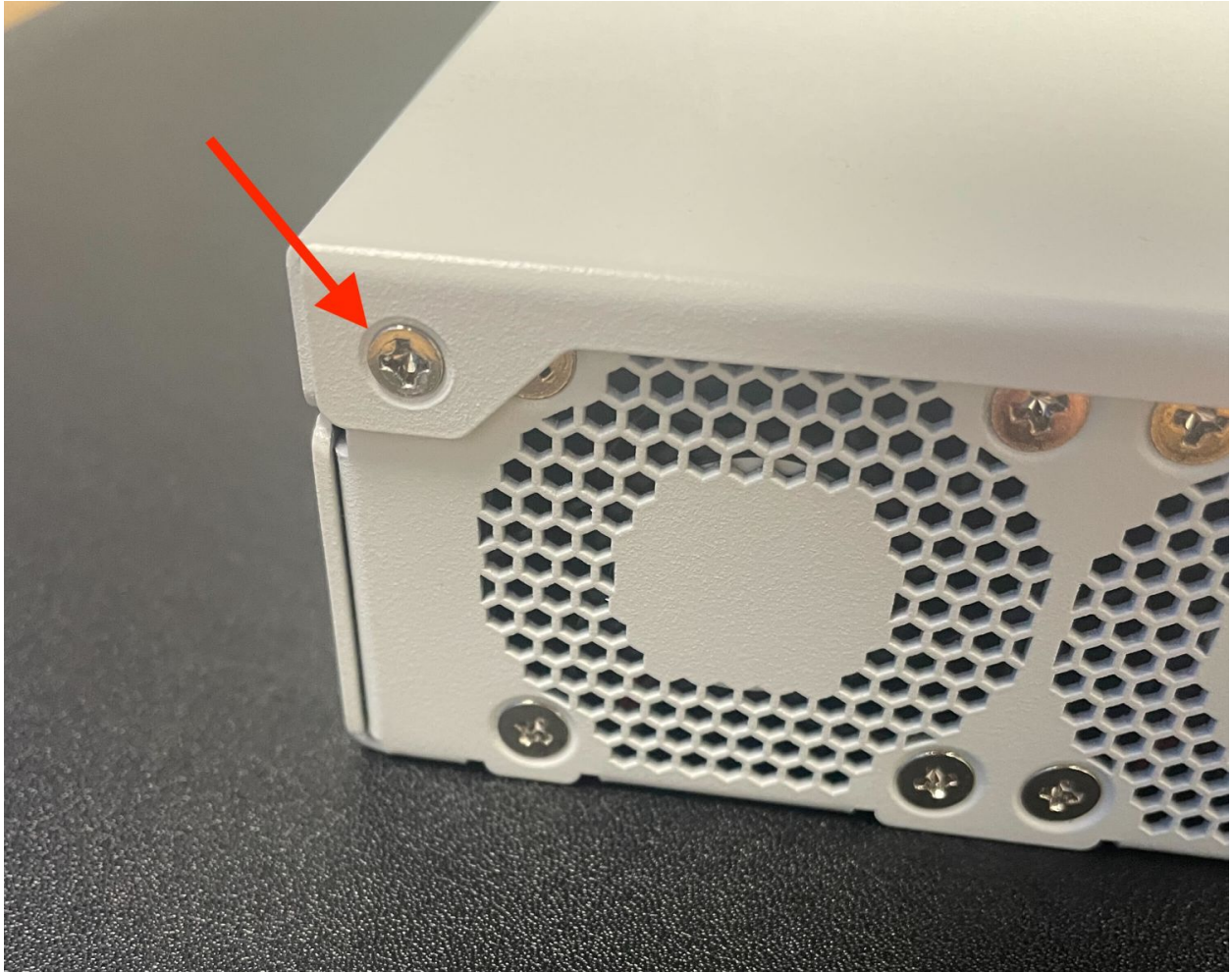


Fig. 60: Screw on the rear side of the unit at the left top corner, indicated with an arrow.

3. Remove the screw from the rear side of the unit at the top right corner using the Phillips head screwdriver.



Fig. 61: Screw on the rear side of the unit at the right top corner, indicated with an arrow.

4. Slide the top cover back away from the front panel until it stops.
5. Lift off the top cover and set it aside, keeping it upright to avoid damaging the top surface.

Remove the Expansion Riser Assembly

The add-on expansion card slots are located on a riser assembly. This riser assembly must be removed from the device to safely add or remove expansion cards.

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. Loosen the two captive screws which attach the riser assembly to the motherboard using the Phillips head screwdriver.



Fig. 62: Sliding back the top cover away from the front panel

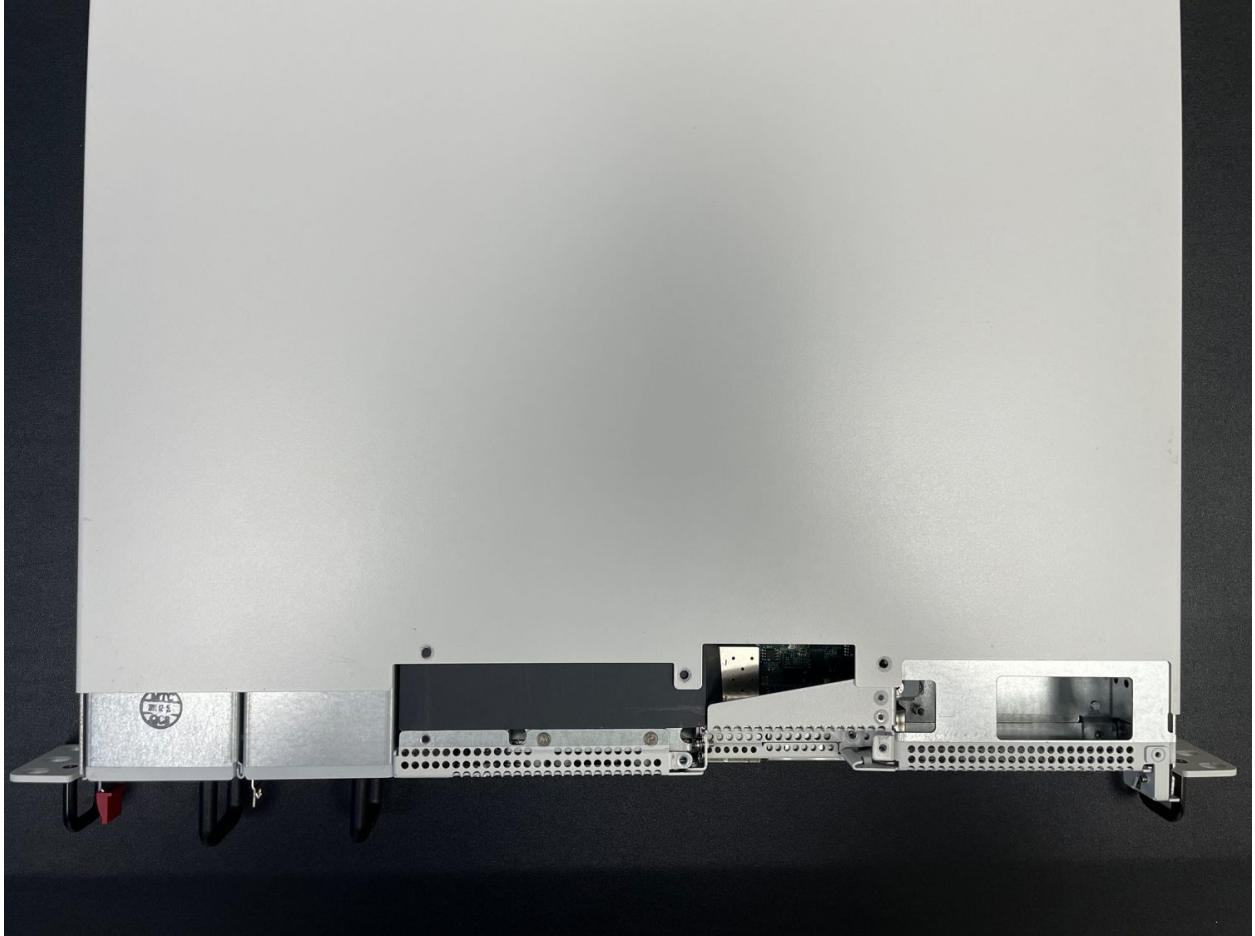


Fig. 63: Top cover in position to be lifted off

Note: These screws are captive and will not fully remove from the riser assembly. It is sufficient to loosen the screws until they no longer attach the riser assembly to the motherboard. This may be felt as a soft “click” when the screw is freely rotating and the threads are not engaged.

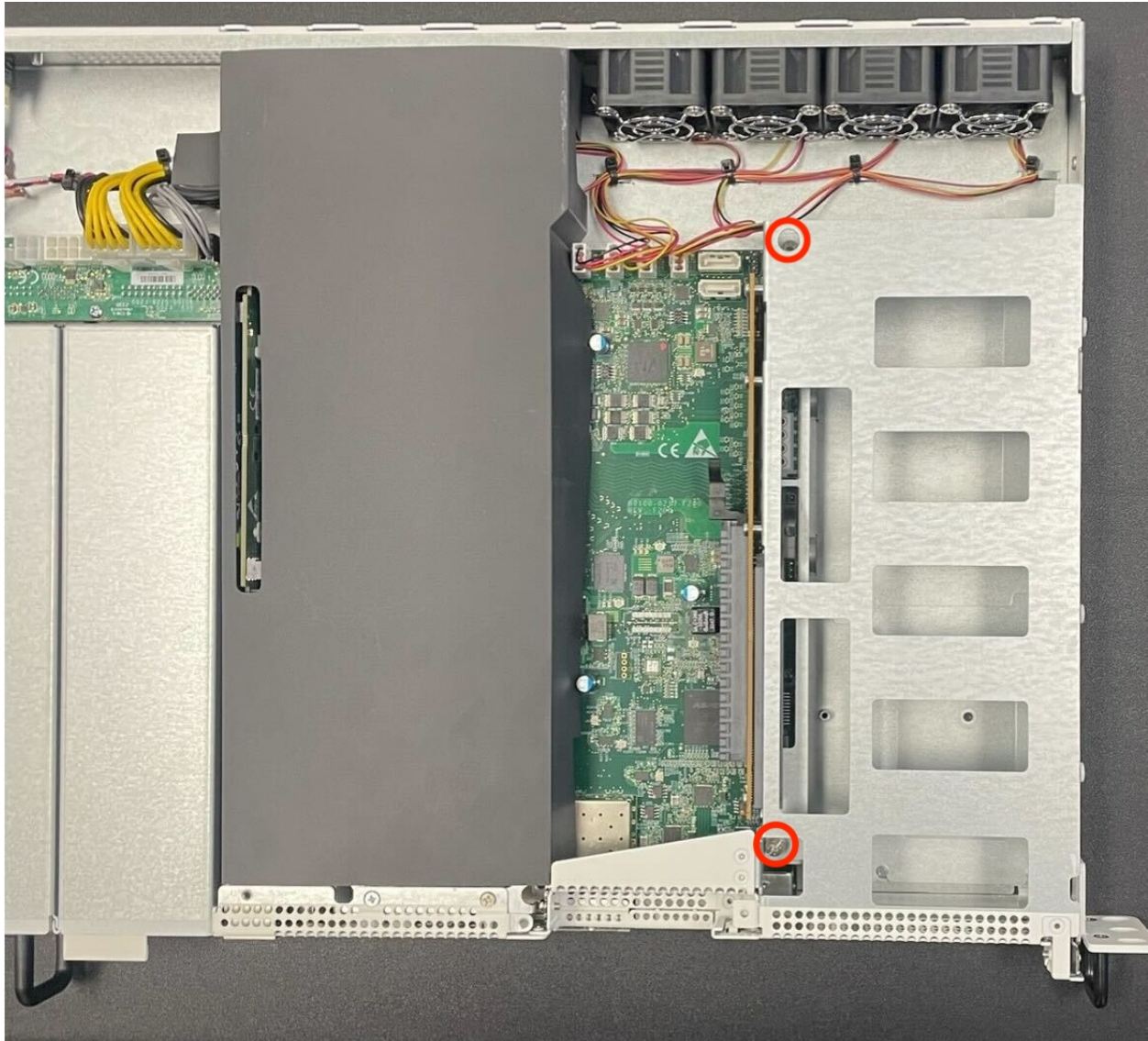


Fig. 64: Location of the captive riser assembly retaining screws indicated with red circles

2. Remove the riser assembly retaining screw on the front of the unit using the Phillips head screwdriver.
3. Carefully lift the riser assembly from the motherboard slot and remove the riser assembly.

Rotating the assembly as seen in figures below can help the removal process with PCIe cards installed.

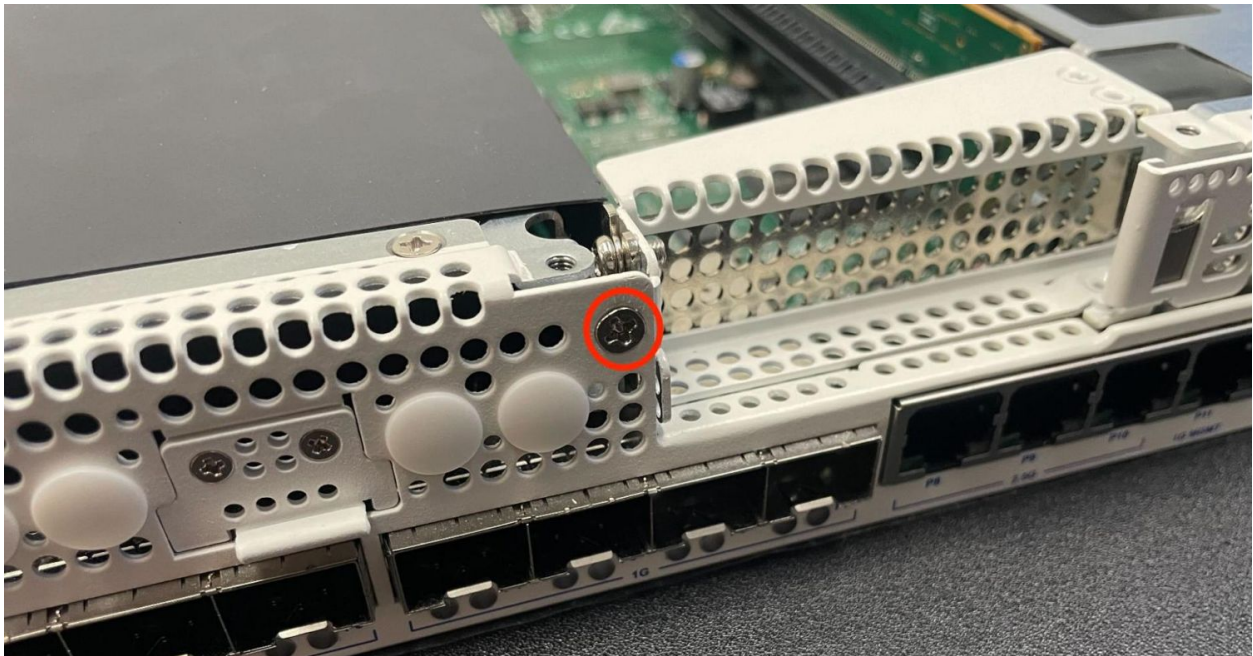


Fig. 65: Location of the riser assembly retaining screw on the front of the unit indicated with a red circle

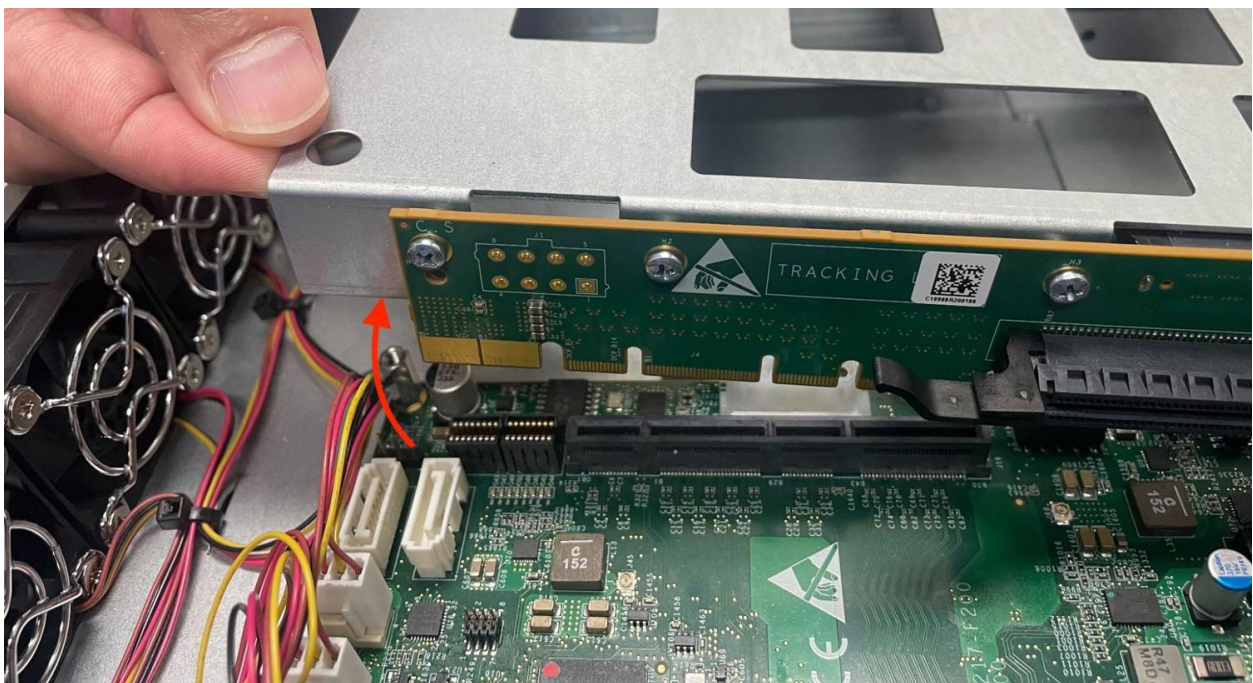


Fig. 66: Lift the riser assembly from the rear to remove it from the riser slot on the motherboard

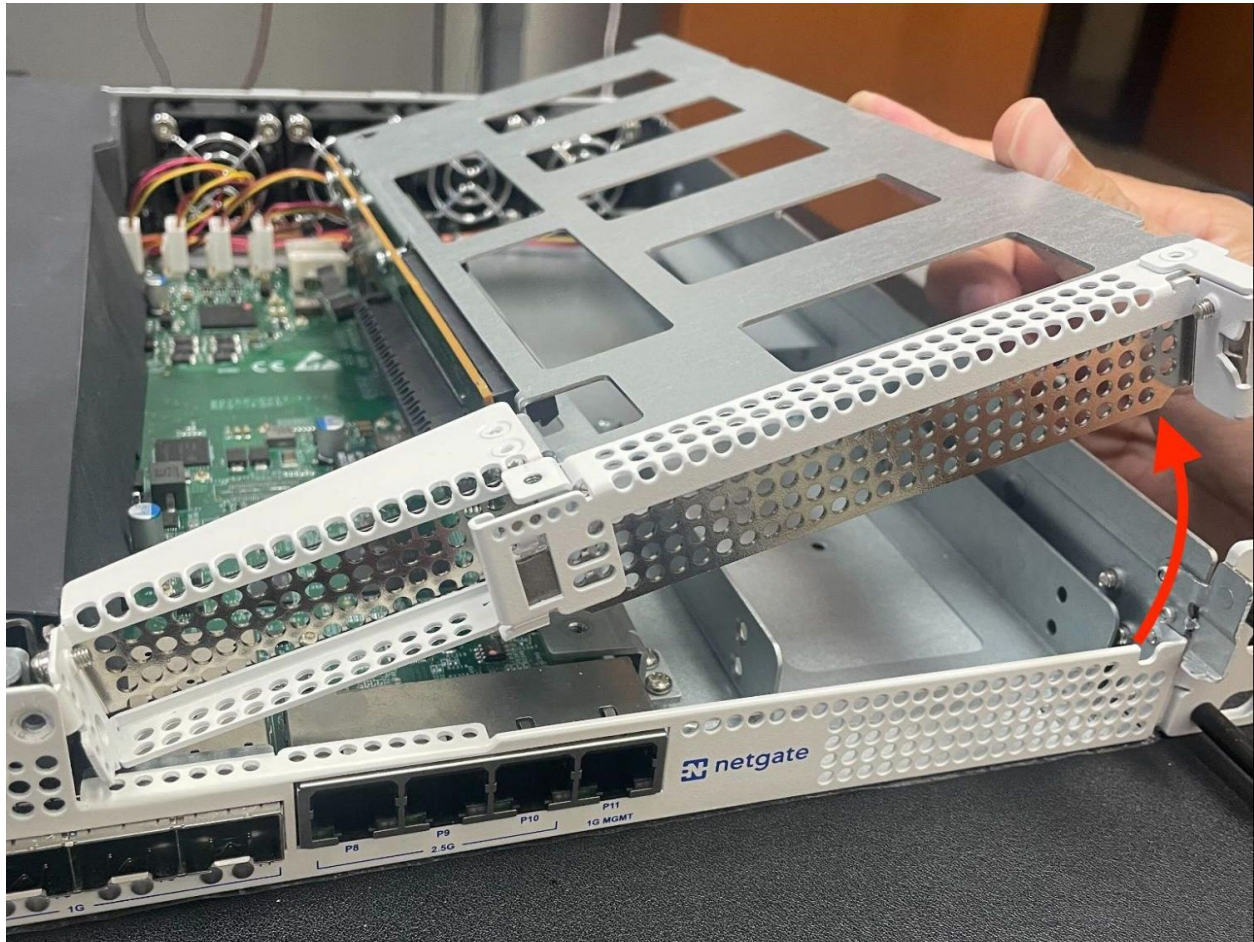


Fig. 67: Lift and rotate the riser assembly from the front as indicated by the red arrow to remove it from the chassis

Install the Add-on Expansion Card

With the riser assembly removed, it is time to install the add-on expansion card.

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 appropriate slot for the expansion card

The expansion slot will vary depending on the card. For example, a card with a low profile bracket would most likely go in the smaller slot on the left, assuming its specifications match the slot capabilities. Some cards have alternate brackets so in those cases it is best to match the card based on its bus requirements, speed, and so on. See [Input and Output Ports](#) for the expansion slot specifications.

2. Loosen or remove the retaining screw from the expansion slot

Tip: It is not typically necessary to fully remove the screw as the card can be moved around it when it is loosened, but removing the screw can make installing or removing the cards easier.

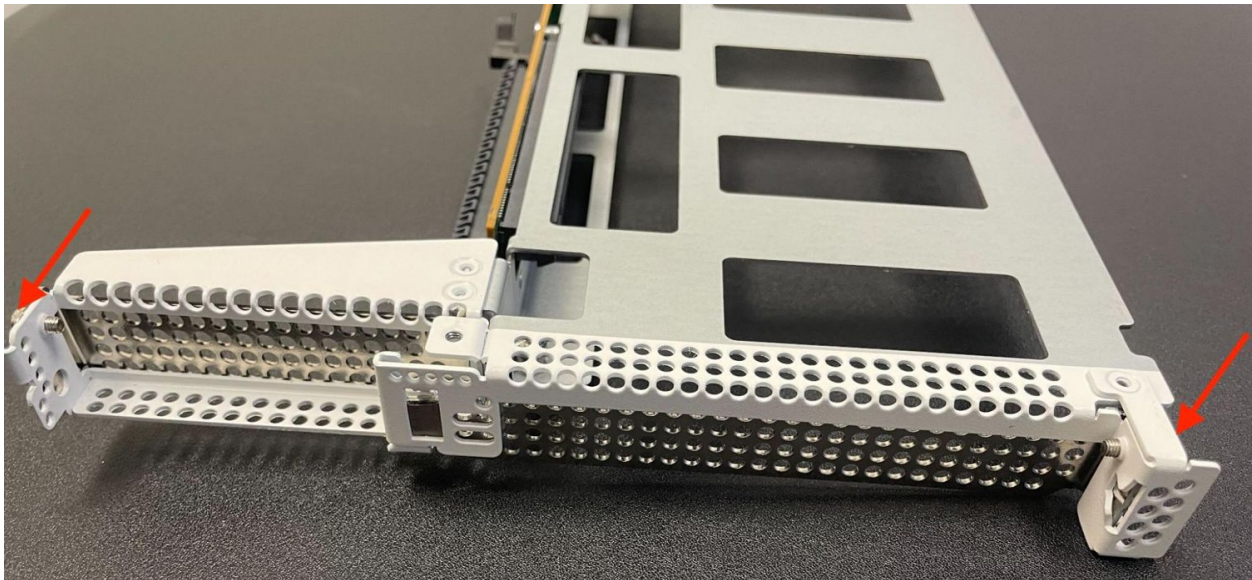


Fig. 68: Location of the add-on expansion card slot retaining screws indicated with red arrows

3. Remove the expansion slot cover by sliding it away from the center of the riser assembly and lifting it out, then set it aside.

Note: The cover will not be necessary so long as there is a card in the expansion slot. Store the cover in a safe place in case it is needed in the future.

4. Install the add-on card into the expansion card slot by sliding it toward the center of the riser assembly until it is fully seated in its socket.
5. Ensure the card is properly aligned and fully inserted into the expansion card slot.

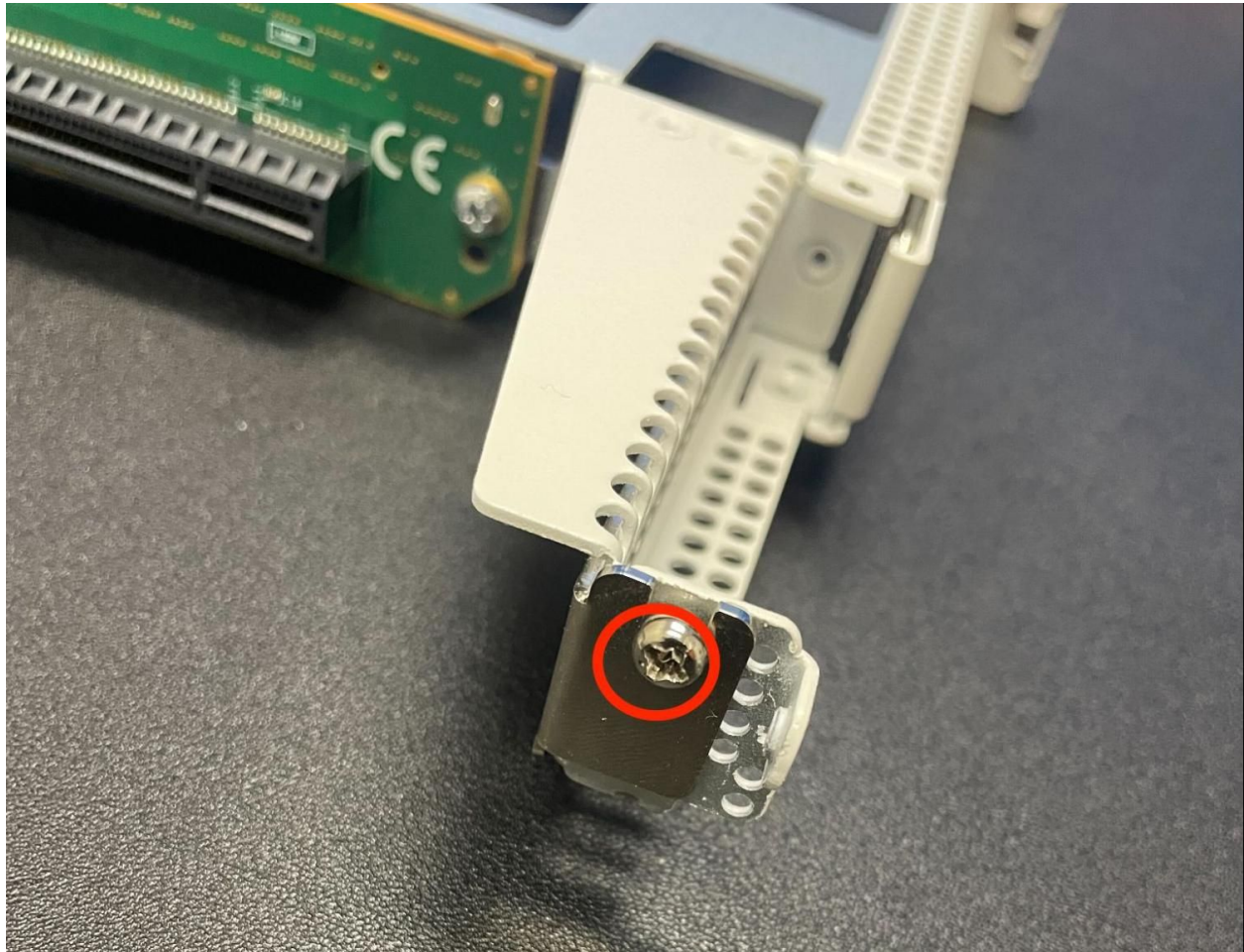


Fig. 69: Location of the low profile add-on expansion card slot retaining screw indicated with a red circle



Fig. 70: Location of the full height add-on expansion card slot retaining screw indicated with a red circle



Fig. 71: Slide the expansion slot cover away from the center of the riser assembly



Fig. 72: Remove the expansion slot cover once it is free from the expansion slot

The rear of the socket has a retention clip to hold the card in place which should be engaged once the card is fully seated

The front of the card should be flush with the front of the riser assembly and aligned with the retention screw hole.

6. Fasten the expansion card to the riser assembly using the retaining screw and the Phillips head screwdriver.

Replace the Riser Assembly

With the expansion card installed in the riser assembly, replace the riser assembly back into the chassis.

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. Insert the riser card back into the chassis and fully seat it into the slot on the motherboard.
2. Replace the riser assembly retaining screw on the front of the unit using the Phillips head screwdriver.
3. Tighten the two captive screws which attach the riser assembly to the motherboard using the Phillips head screwdriver.

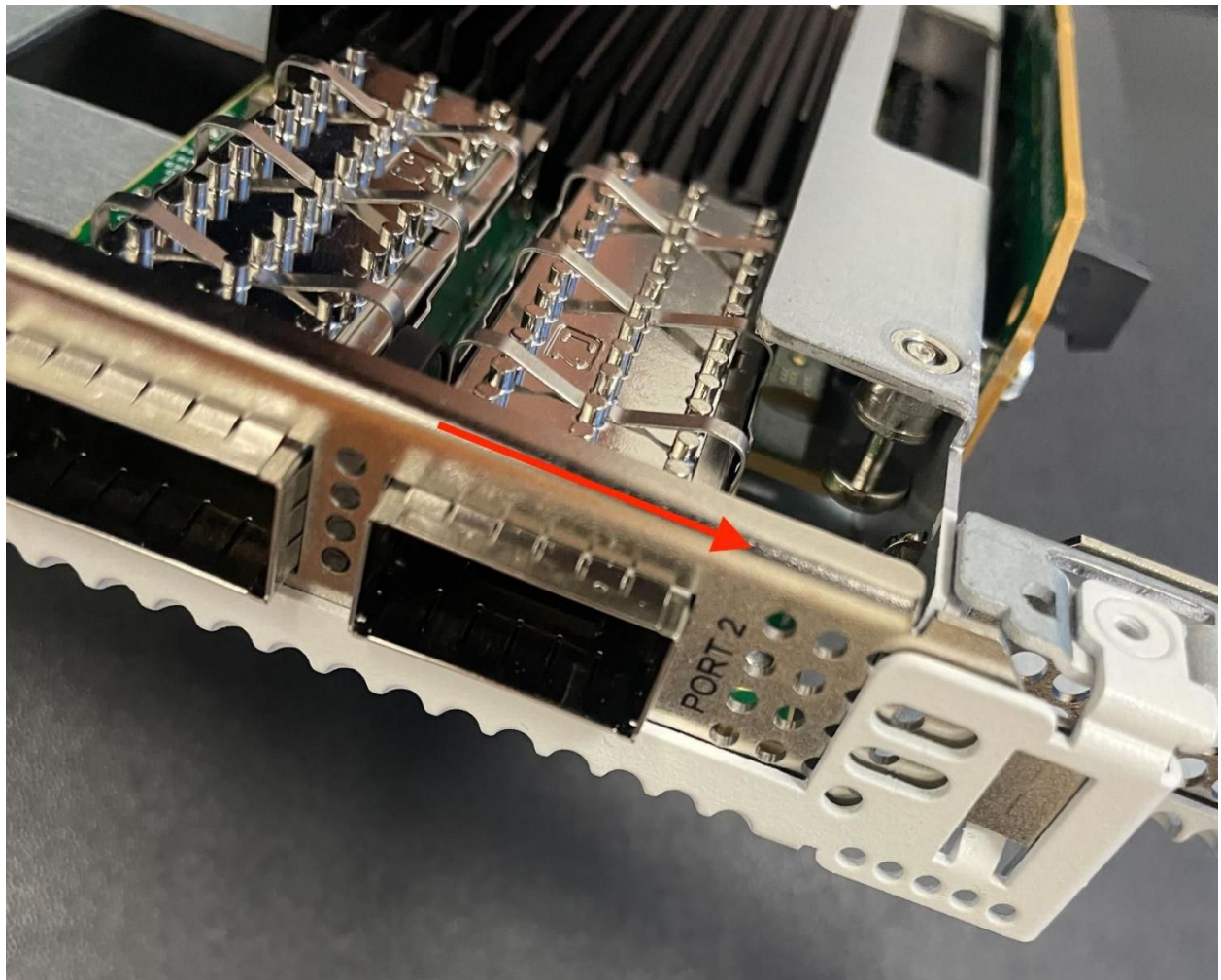


Fig. 73: Installing an add-on network interface card into an expansion slot

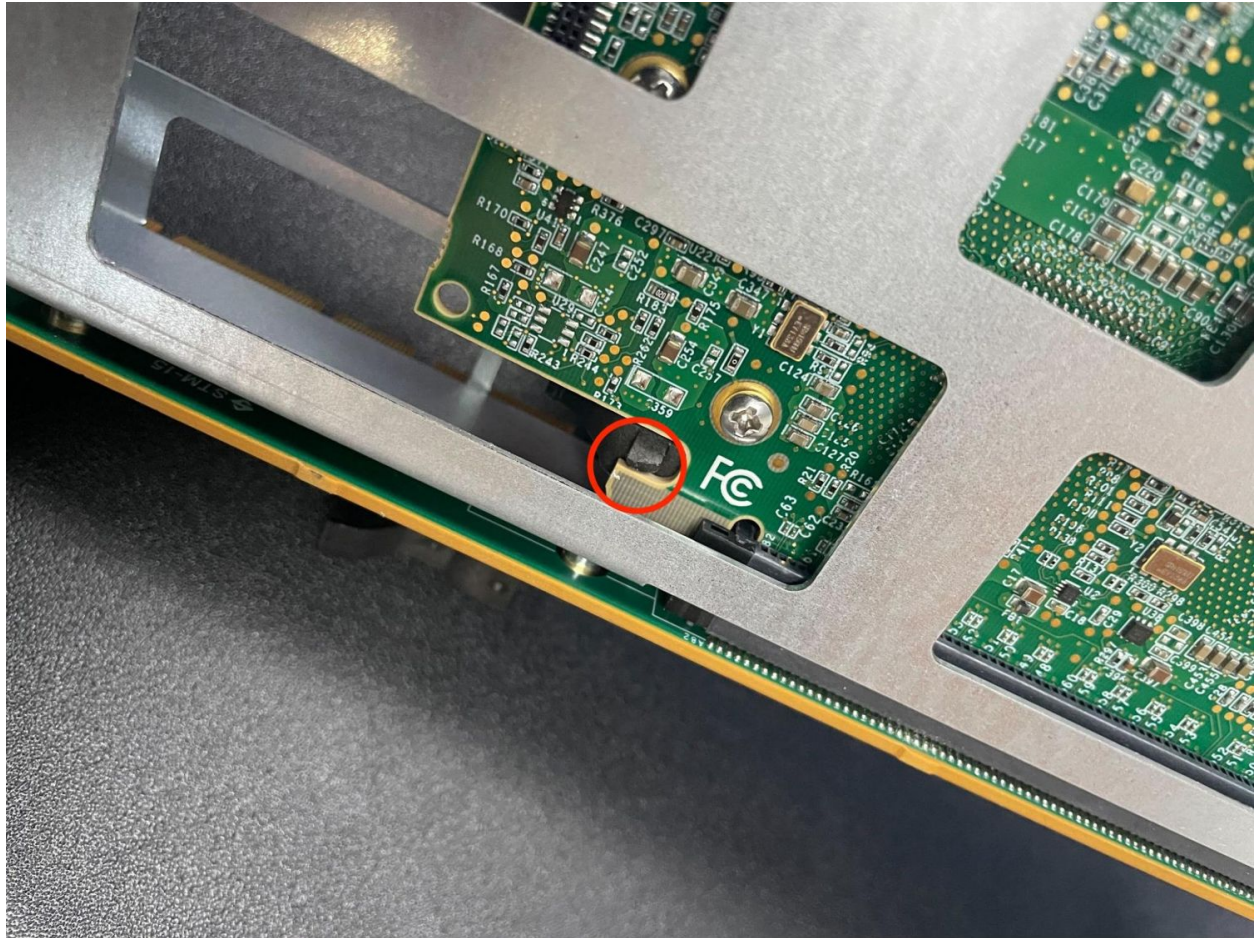


Fig. 74: Expansion card slot retention clip holding a card in place

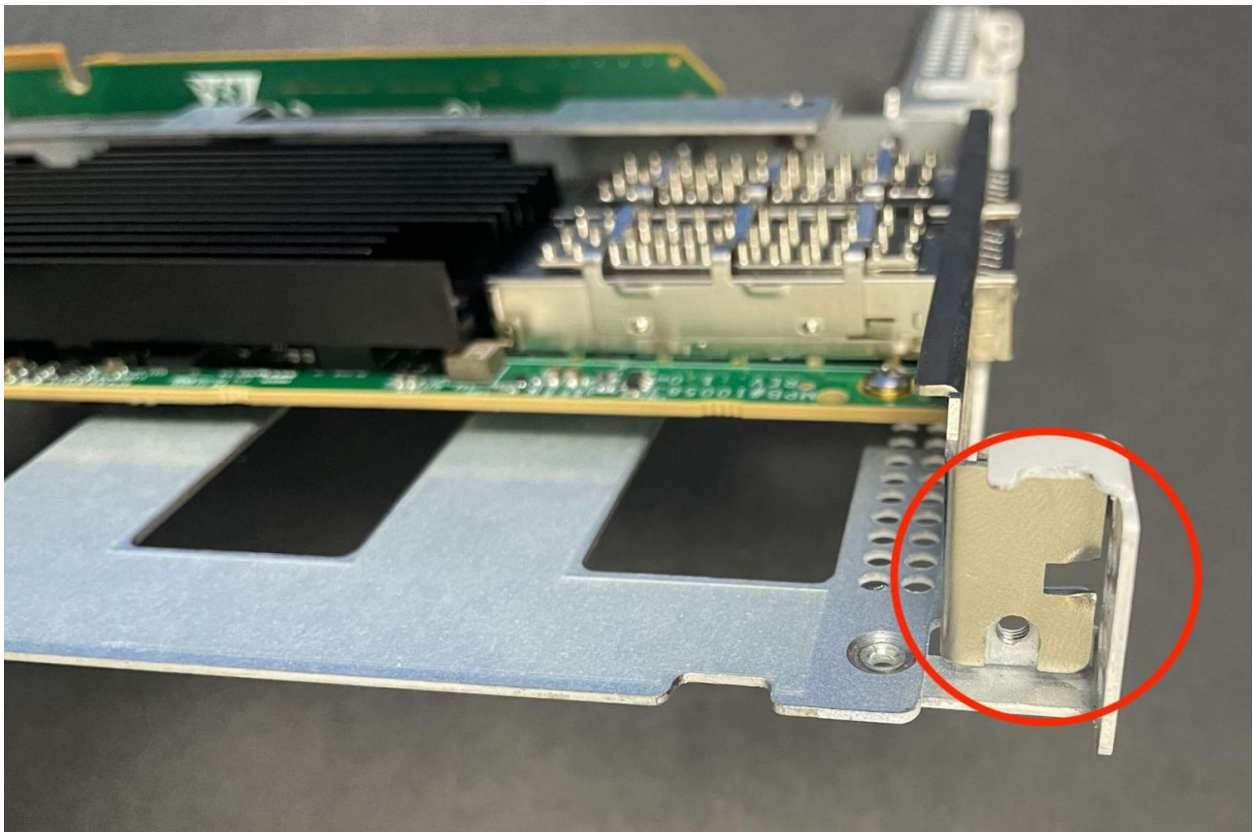


Fig. 75: Expansion card aligned with the riser assembly and retention screw hole

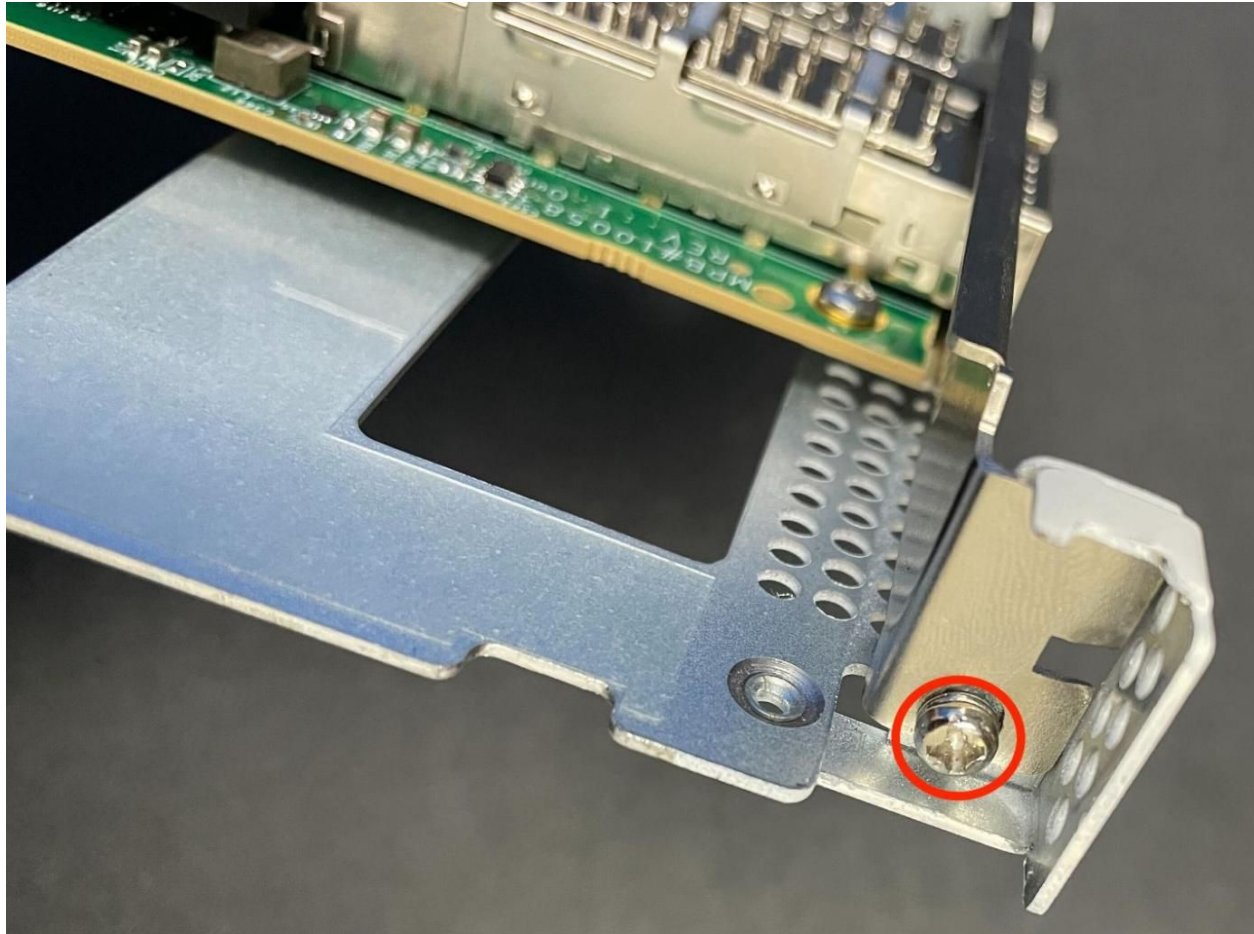


Fig. 76: Expansion card fastened in the riser assembly using the retention screw

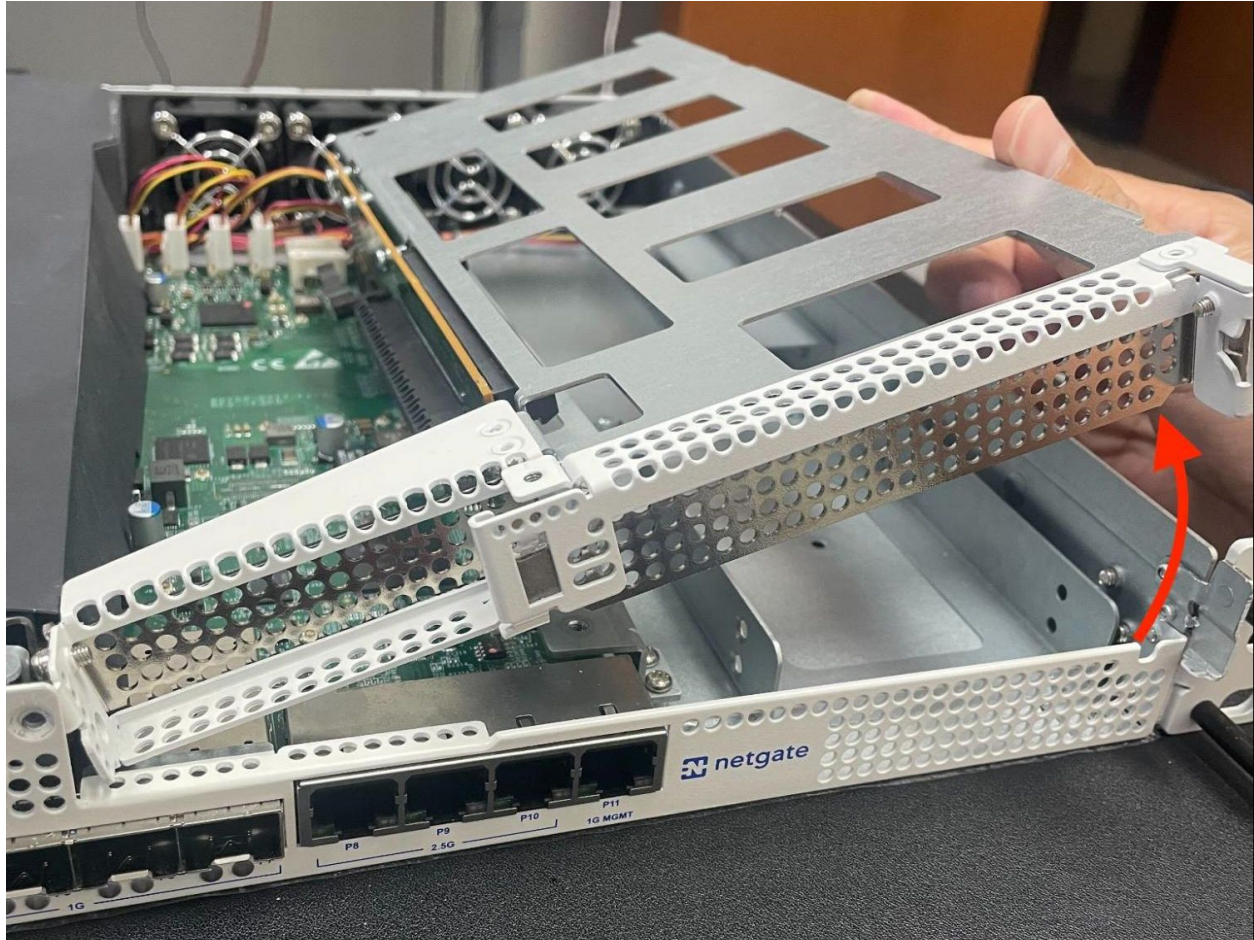


Fig. 77: Rotate and replace the riser assembly from the front in the **opposite** direction indicated by the red arrow

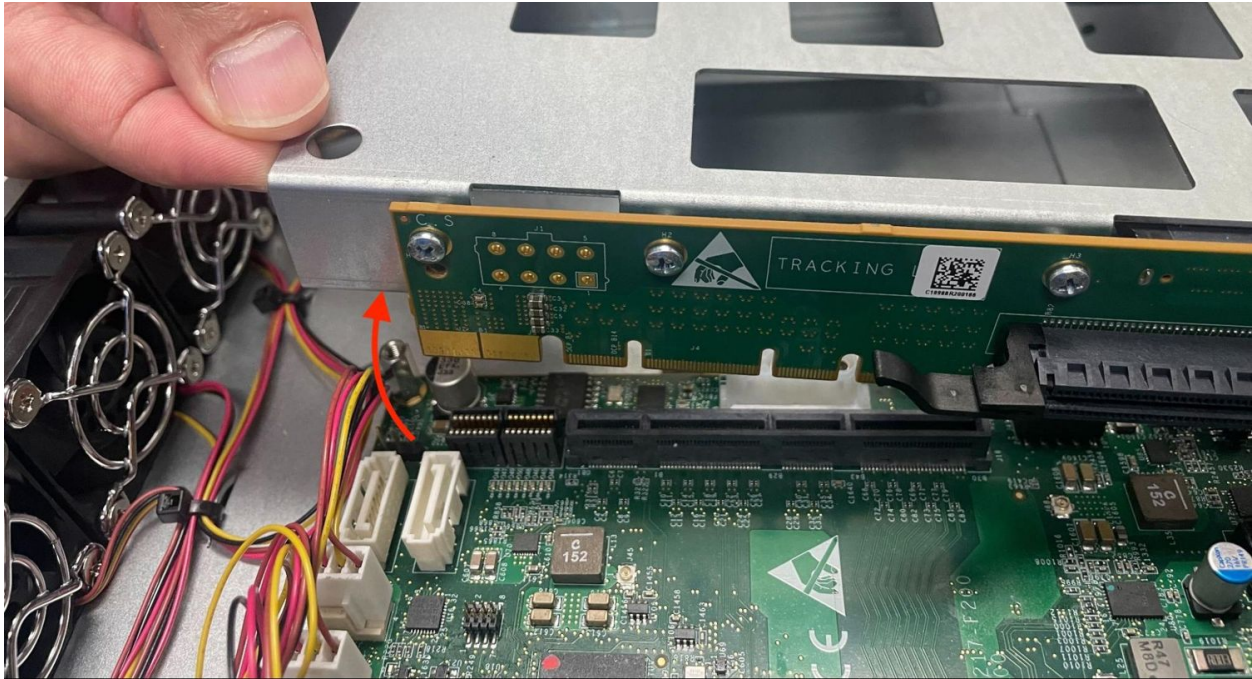


Fig. 78: Re-seat the riser assembly in the the riser slot from the rear of the motherboard in the **opposite** of the direction indicated by the red arrow

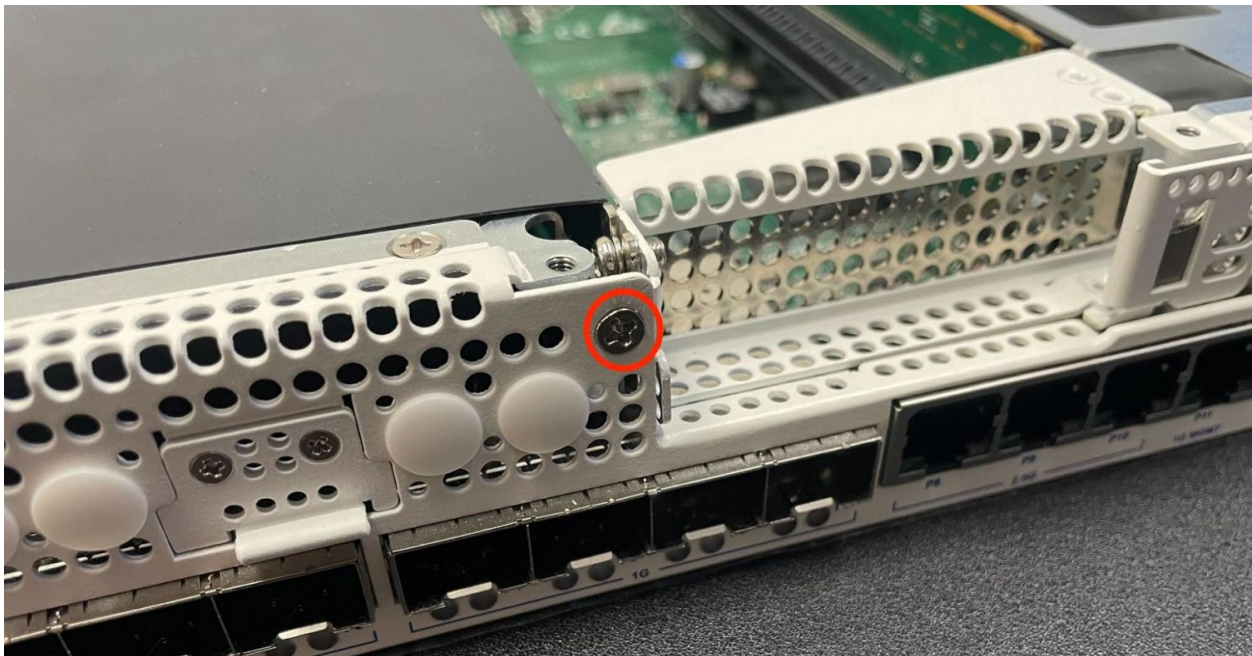


Fig. 79: Location of the riser assembly retaining screw on the front of the unit indicated with a red circle

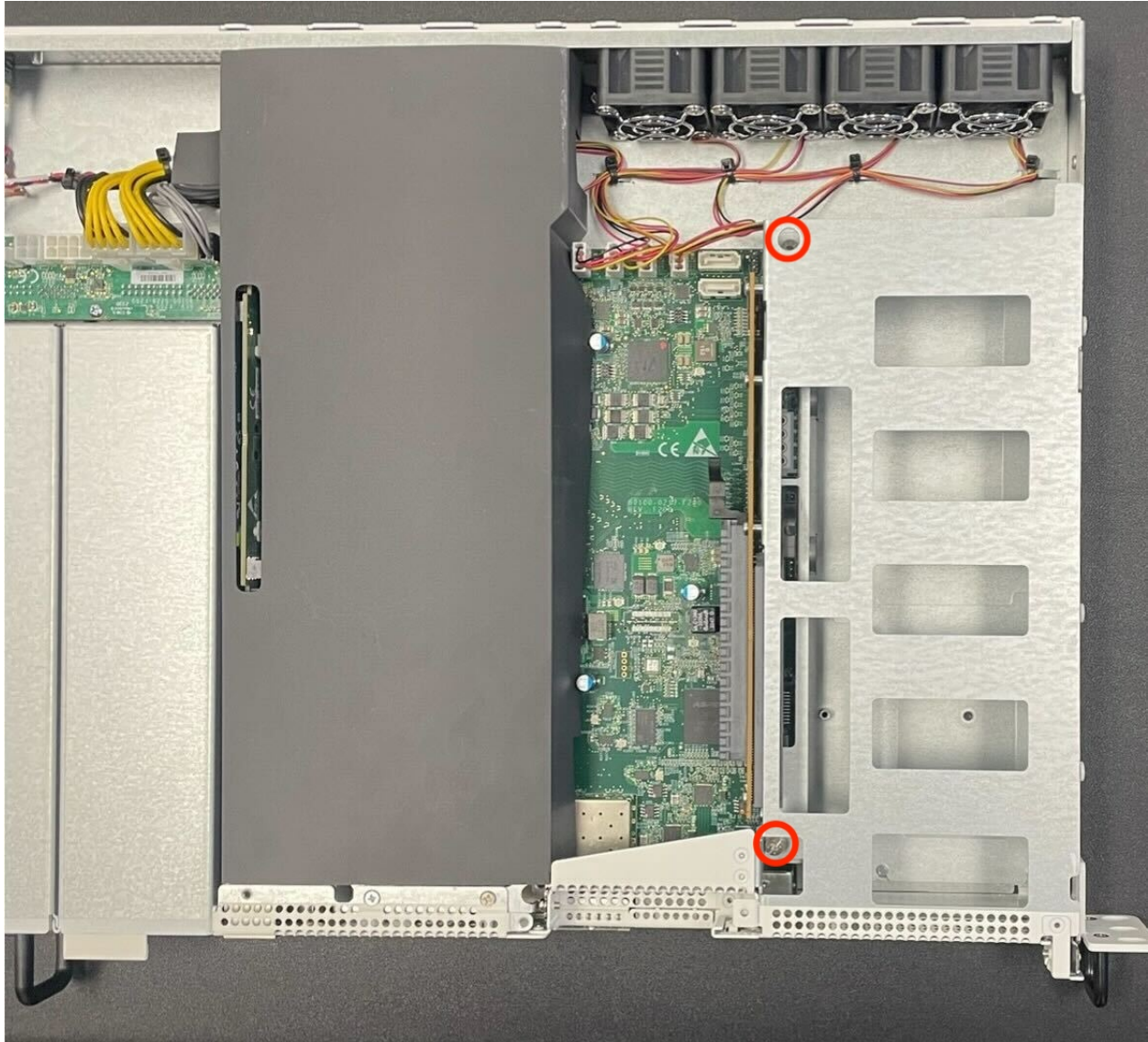


Fig. 80: Location of the captive riser assembly retaining screws indicated with red circles

Replacing and Fastening the Lid

With the internal components all in place, the next step is to replace the lid and all its 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 top cover with the top of the unit, a short distance behind the front panel.

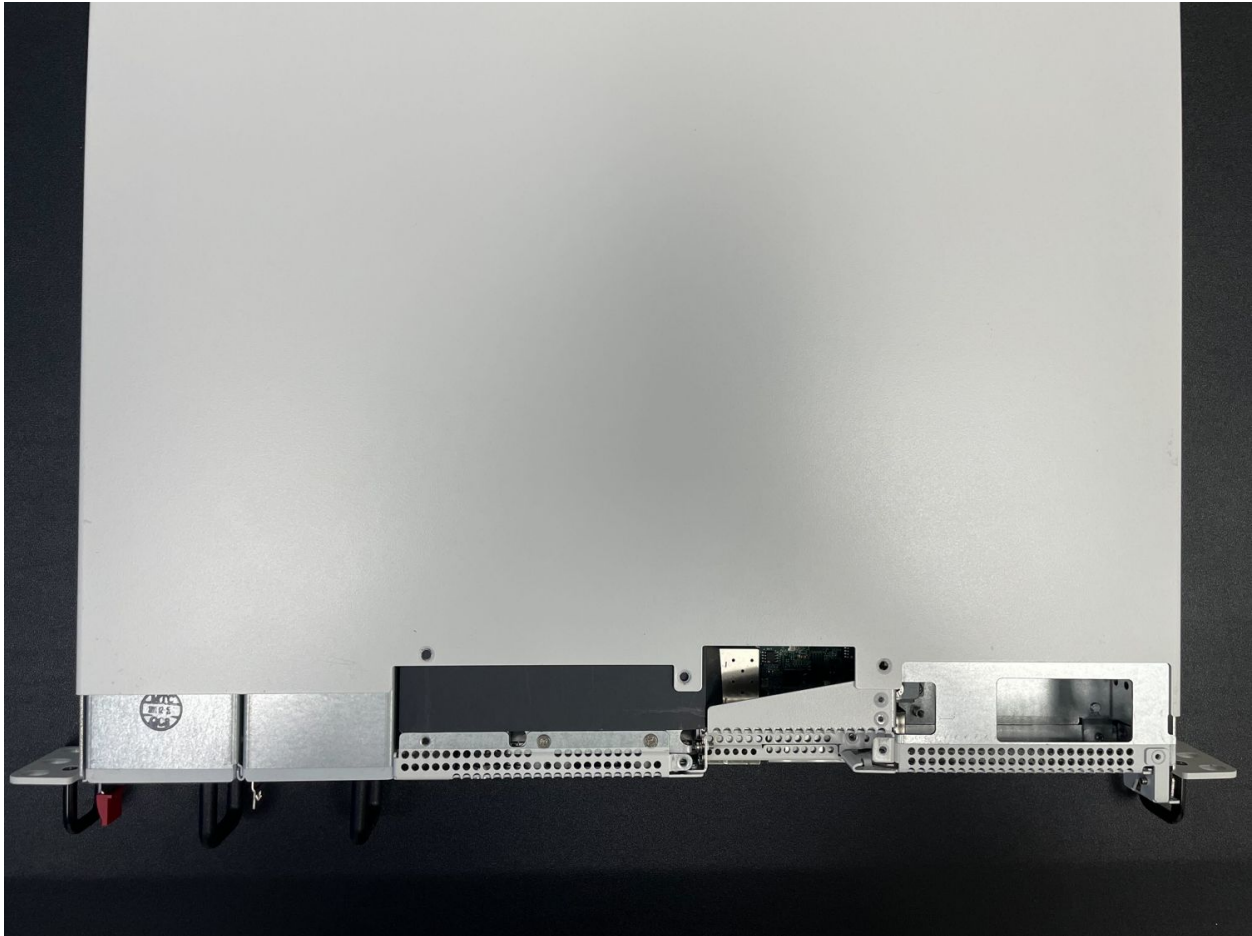


Fig. 81: Top cover in position to be replaced

2. Slide the top cover toward the front of the unit into its closed position.

Replace the screws on the rear of the unit (left and right top corners) using the Phillips head screwdriver.

Replace the screws on the top of the unit using the Phillips head screwdriver.



Fig. 82: Slide the top cover back toward the front panel

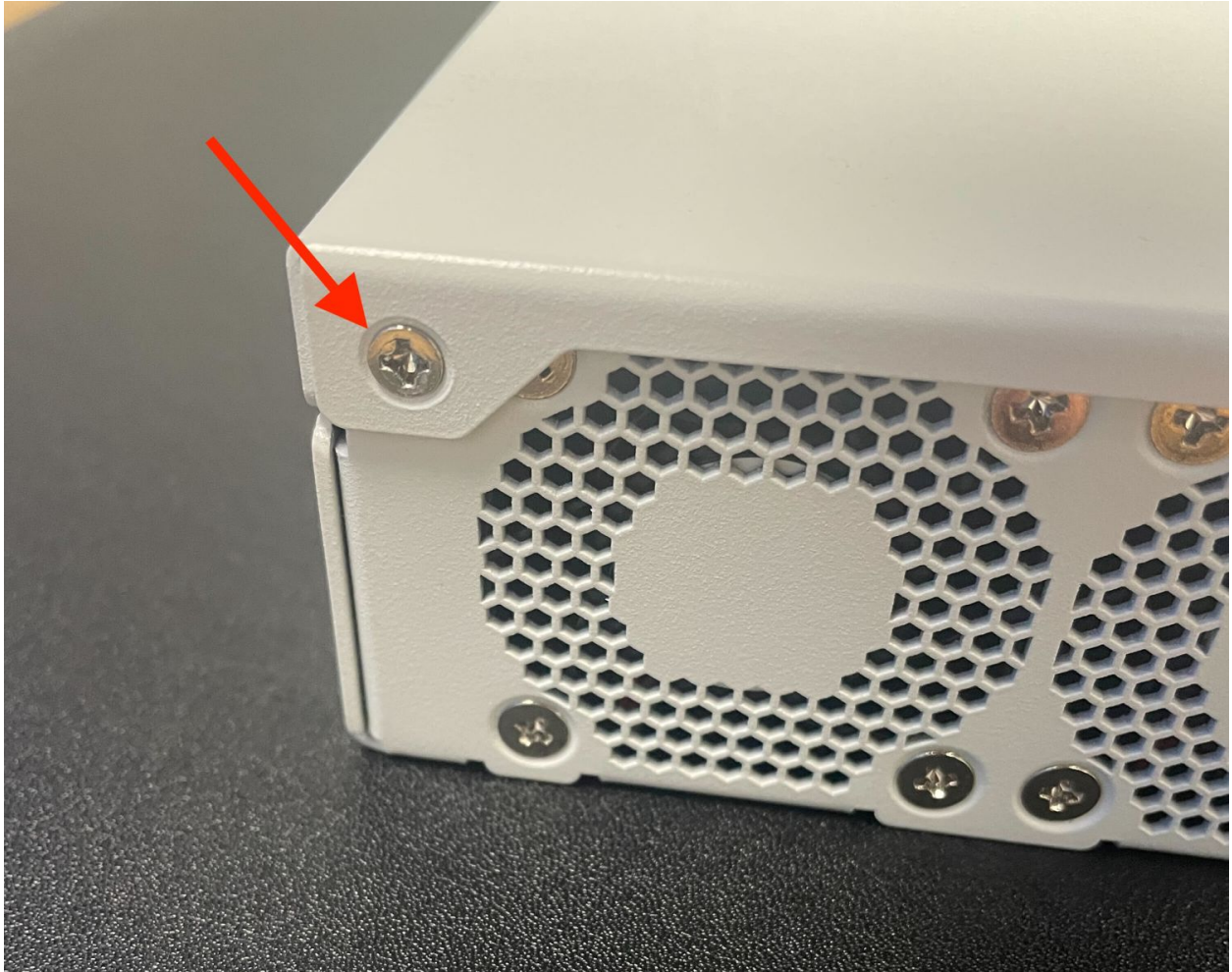


Fig. 83: Screw on the rear side of the unit at the left top corner, indicated with an arrow.



Fig. 84: Screw on the rear side of the unit at the right top corner, indicated with an arrow.

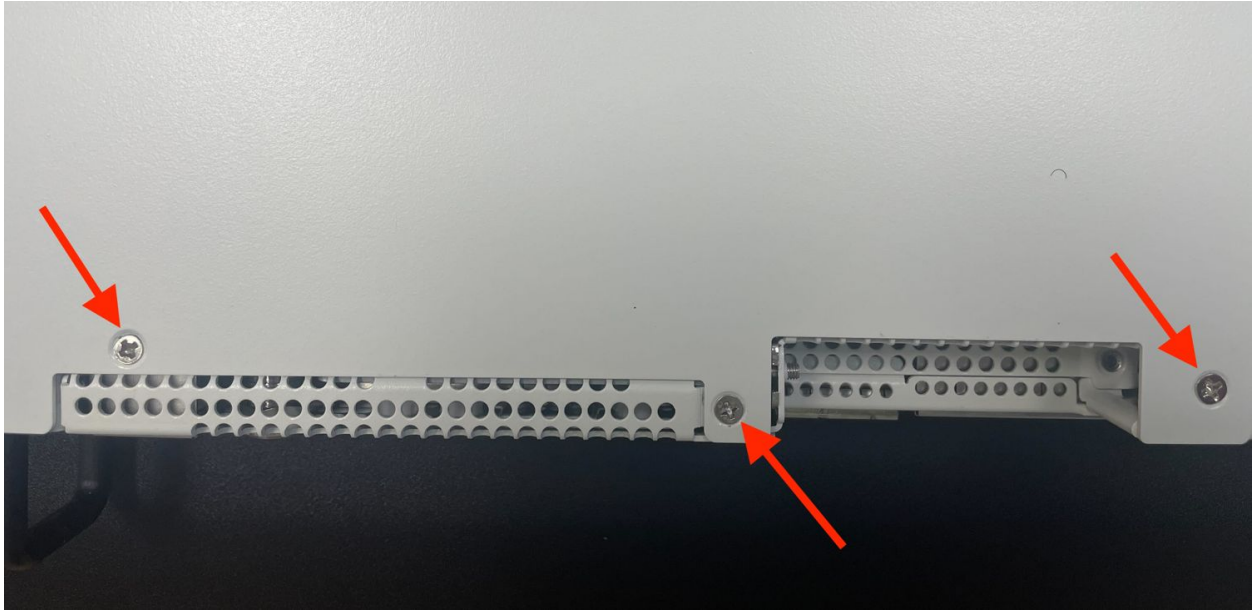


Fig. 85: Screws on the top of the cover at the front of the unit, indicated with arrows

Reconnect

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

1. Mount the Netgate 8300 in the rack
2. Plug in all network cables, USB cables and devices, serial console connections, etc.
3. Insert the USB memstick containing the installation media
4. Plug the power cables into all installed power supply units.
5. Turn power on to the unit by changing the power switch on the rear of the unit to the **on** position.
6. Reconnect to the serial console

Reassign Interfaces (Network Interface Cards Only)

If the expansion card added to the device is a network interface card, this must be accounted for in pfSense software once the card is in place.

If the network card **does not** utilize the same driver as the interfaces in the base system (`ice(4)`), then the interfaces can be assigned and enabled as needed based on the information in the [pfSense software documentation for interfaces](#).

Network interface cards which use **the same driver** as built-in ports on the device (`ice(4)`) **will** cause the existing interface assignments to **shift**, which **will negatively impact** connectivity as the interfaces for WAN, LAN, and so on will suddenly be mapped to different physical ports.

There are multiple ways to work around this, depending on the state of the installation on the device.

If this is a new device or if it has no configuration that needs retained, then the easiest way to properly reassign the interfaces is to either perform a factory reset ([Factory Reset Procedure](#)) or reinstall pfSense Plus software ([Reinstalling pfSense Plus Software](#)). Either of those actions will take these expansion card(s) into account when pfSense Plus software automatically assigns the interfaces on a default configuration.

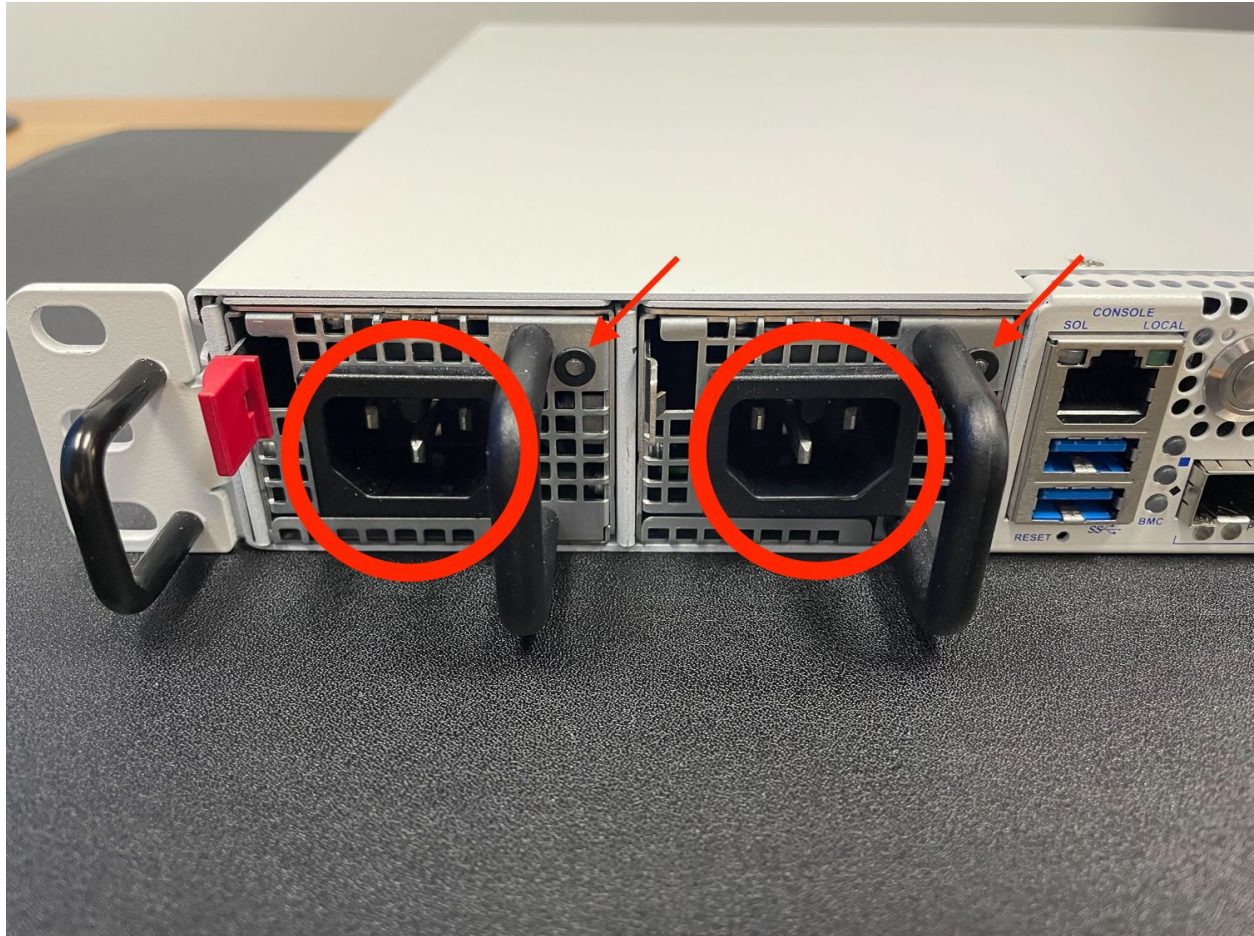


Fig. 86: Power Supply Units with power receptacles circled and status LEDs indicated with arrows

See also:

See [Networking Ports](#) for details.

If the device has an existing configuration which must be adjusted to match the new interface layout, then the ports must be reassigned manually. Since GUI access is likely broken by the interfaces being moved, this may need to be performed at the console. For simple configurations this may be viable, but for more complicated configurations involving LAGG, VLANs, and so on it may be difficult.

Another option is to edit the configuration backup and adjust the interfaces manually, then perform a factory reset ([Factory Reset Procedure](#)) or reinstall pfSense Plus software ([Reinstalling pfSense Plus Software](#)) and restore the adjusted configuration.

See also:

[Netgate TAC](#) may be able to assist with adjusting configurations for customers in many cases.

Re-arm the Intrusion Sensor

Opening the case to install the expansion card will trigger the intrusion alarm sensor, even while the device is removed from power. The intrusion alarm causes the fans to run at a higher fixed speed until the sensor is re-armed.

Once pfSense software is up and running, follow the procedure in [Re-arm the Chassis Intrusion Switch](#) to reset the sensor.

2.12 Slide Rail Installation

The Netgate 8300 has an optional set of [slide rails available for purchase](#) in the [Netgate Store](#).

For information on how to install and operate the rails, download and read the following guide:

[Netgate 8300 Slide Rail Install Guide](#)

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 support and improve your customer satisfaction; Netgate training has got you covered.

<https://www.netgate.com/training>

3.1.2 Resource Library

To learn more about how to use 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

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

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

3.1.4 Community Options

Customers who elected not to get a [paid support plan](#), can find help from the active and knowledgeable pfSense software community on the Netgate forum.

<https://forum.netgate.com/>

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](#).