Security Gateway Manual

XG-1537

Jan 08, 2024

CONTENTS

This Quick Start Guide covers the first time connection procedures for the Netgate® 1537 1U Firewall Appliance and will provide the information needed to keep the appliance up and running.

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

CHAPTER

ONE

OUT OF THE BOX

1.1 Getting Started

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

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

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

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

The next step is to connect the LAN port (shown in the *Input and Output Ports* section) of the Netgate appliance to the computer which will be used to access the firewall console.

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

1.1.1 Initial Setup

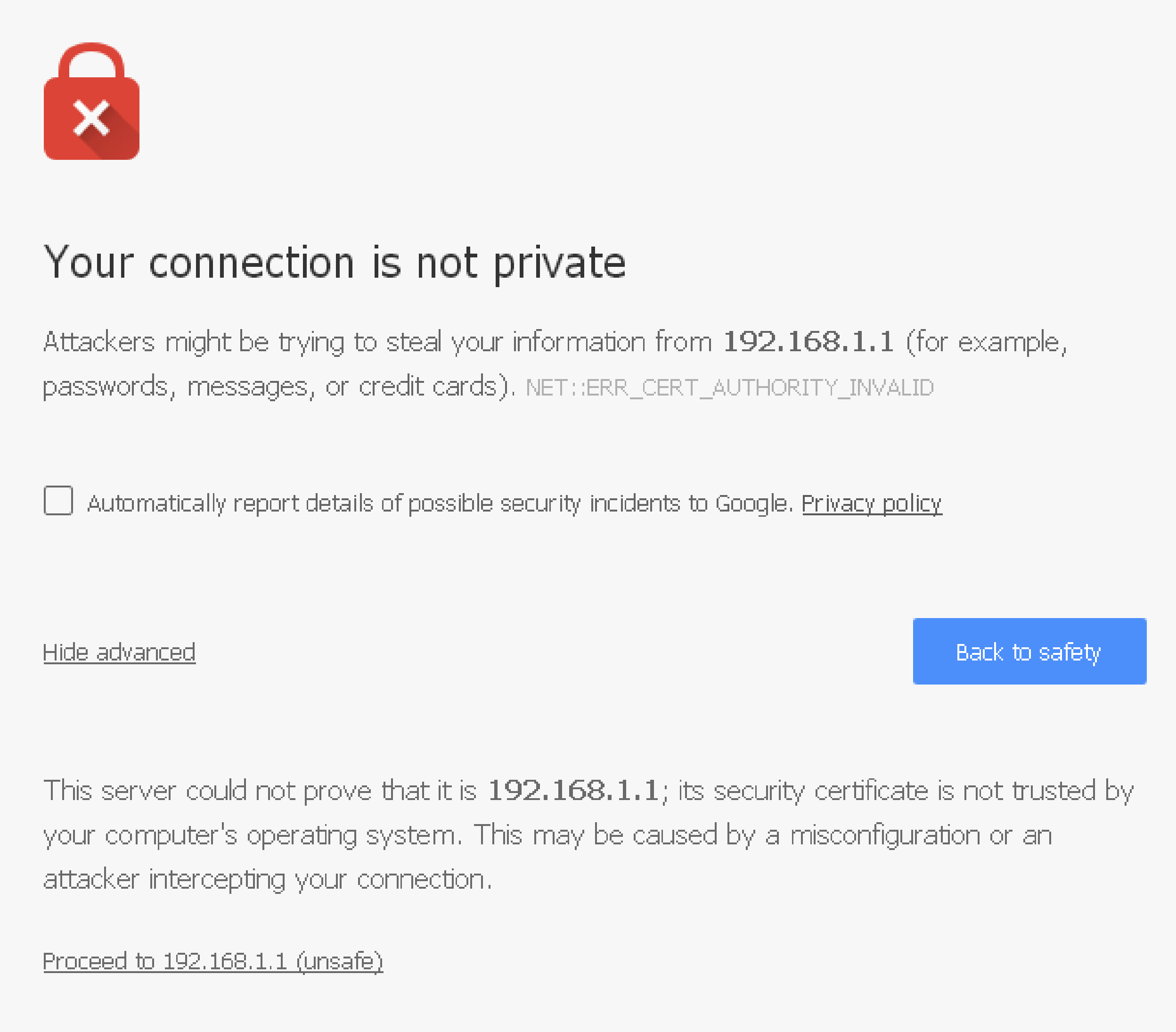
The next step is to power up the modem and the firewall. Plug in the power supply to the power port (shown in the *Input and Output Ports* section).

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

Once the Netgate appliance is booted, the attached computer should receive a `192.168.1.x` IP address via DHCP from the Netgate appliance.

1.1.2 Logging Into the Web Interface

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



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). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

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)

At the login page enter the default password and username:

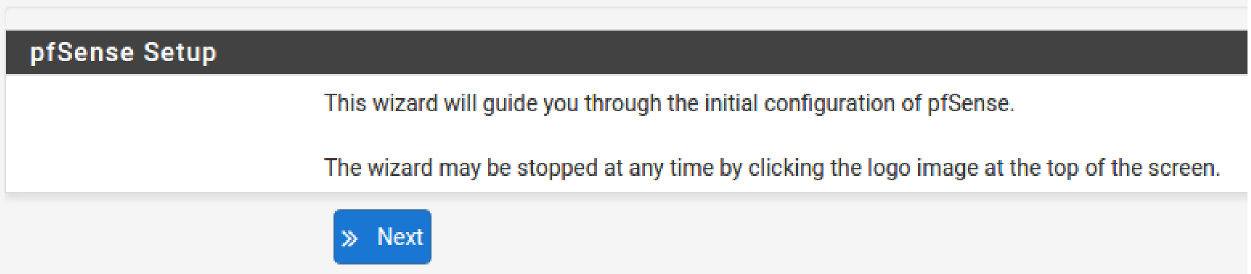
Username `admin`

Password `pfsense`

Click **Login** to continue

1.1.3 Wizard

Upon successful login, the GUI displays the following

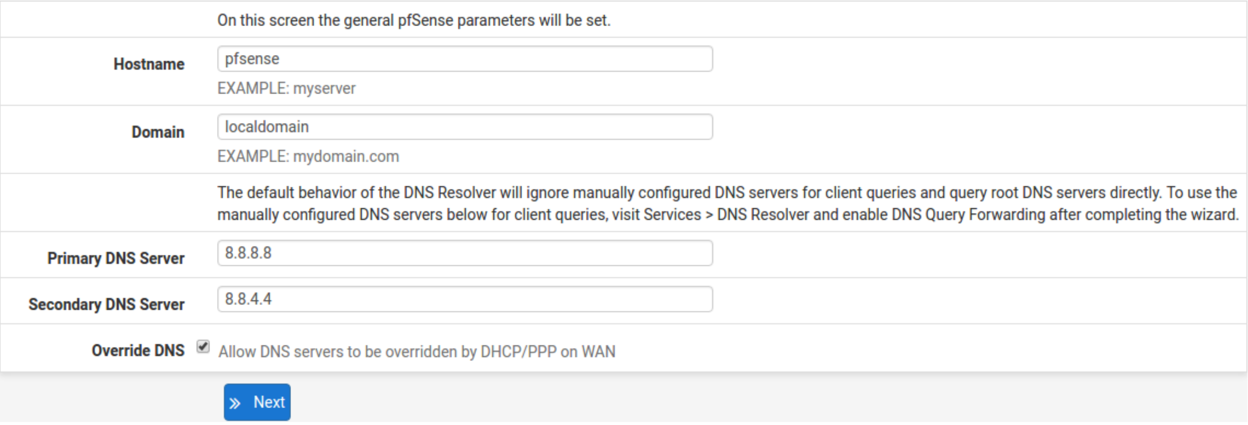


pfSense Setup

This wizard will guide you through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

1.1.4 Configuring Hostname, Domain Name and DNS Servers



	On this screen the general pfSense parameters will be set.
Hostname	pfsense EXAMPLE: myserver
Domain	localdomain 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	8.8.8.8
Secondary DNS Server	8.8.4.4
Override DNS	☑ Allow DNS servers to be overridden by DHCP/PPP on WAN

1.1.5 Hostname

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

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

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

1.1.6 Domain

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

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

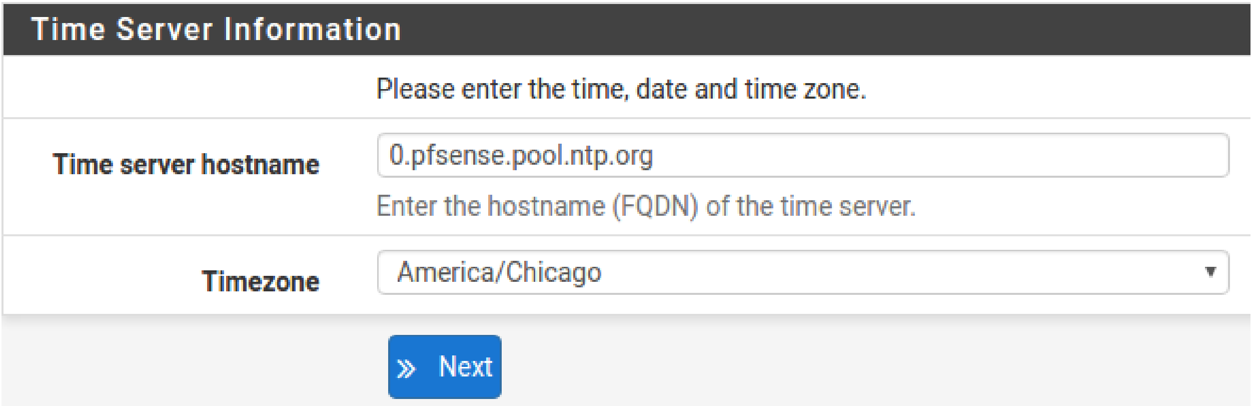
1.1.7 DNS Servers

The DNS server fields can be left blank if the DNS Resolver will be left in the default non-forwarding mode. The settings may also be left blank if the WAN connection is using DHCP, PPTP or PPPoE types of Internet connections and the ISP automatically assigns DNS server IP addresses.

If using the DNS Resolver in forwarding mode or the DNS forwarder combined with a static IP address on WAN, DNS server IP addresses must be entered here for name resolution to function.

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

1.1.8 Time Server Configuration



Time Server Information

Please enter the time, date and time zone.

Time server hostname: 0.pfsense.pool.ntp.org

Enter the hostname (FQDN) of the time server.

Timezone: America/Chicago

1.1.9 Time Server Synchronization

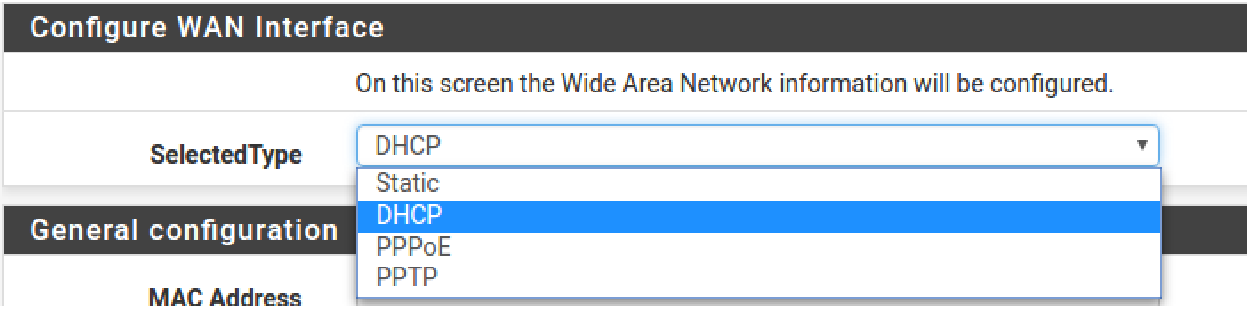
Setting time server synchronization is quite simple. The best practice is to use the default time server address, which will randomly select several NTP servers from a pool.

1.1.10 Setting Time Zone

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

1.1.11 Configuring Wide Area Network (WAN) Type

The WAN interface type is the next to be configured. The IP address assigned to this section becomes the Public IP address that this network will use to communicate with the Internet.



Configure WAN Interface

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

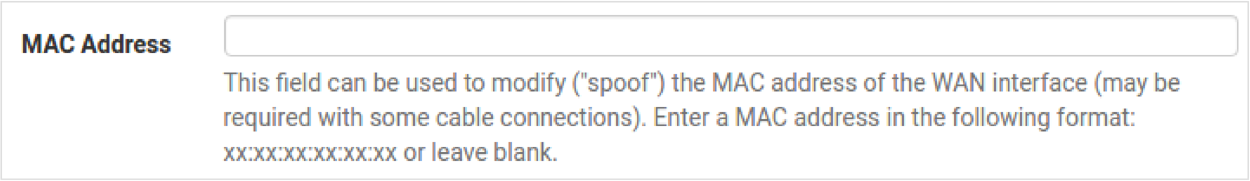
SelectedType: DHCP

This depicts the four possible WAN interface types. Static, DHCP, PPPoE and PPTP. One must be selected from the drop-down list.

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

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

1.1.12 MAC Address



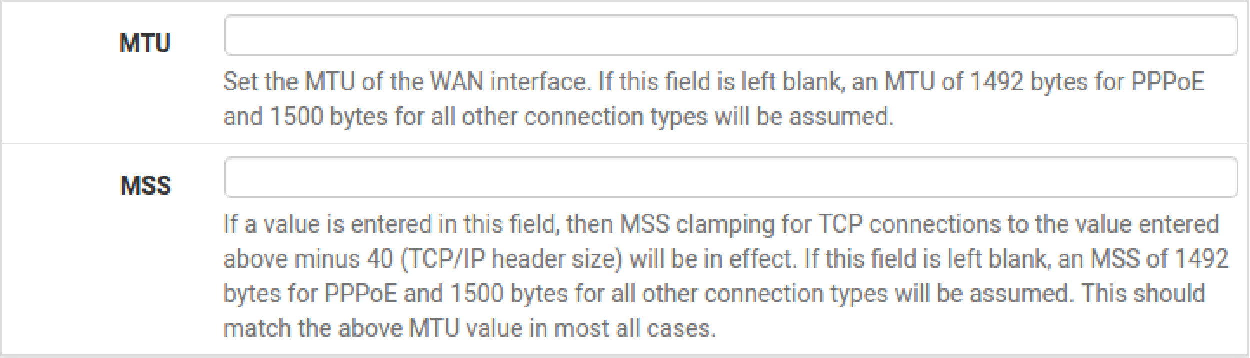
MAC Address

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.

If replacing an existing firewall on an ISP that strictly controls MAC address changes, the WAN MAC address of the old firewall may be entered here, if it can be determined. This is typically unnecessary but it can help avoid temporary issues involved in switching out firewalls, such as ARP caches, ISPs locking to single MAC addresses, etc.

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

1.1.13 Configuring MTU and MSS



MTU

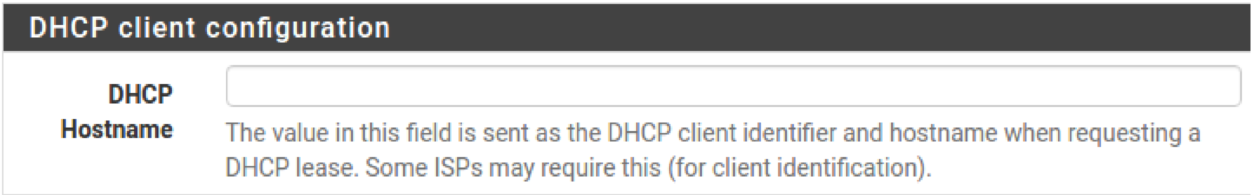
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

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.

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

1.1.14 Configuring DHCP Hostname

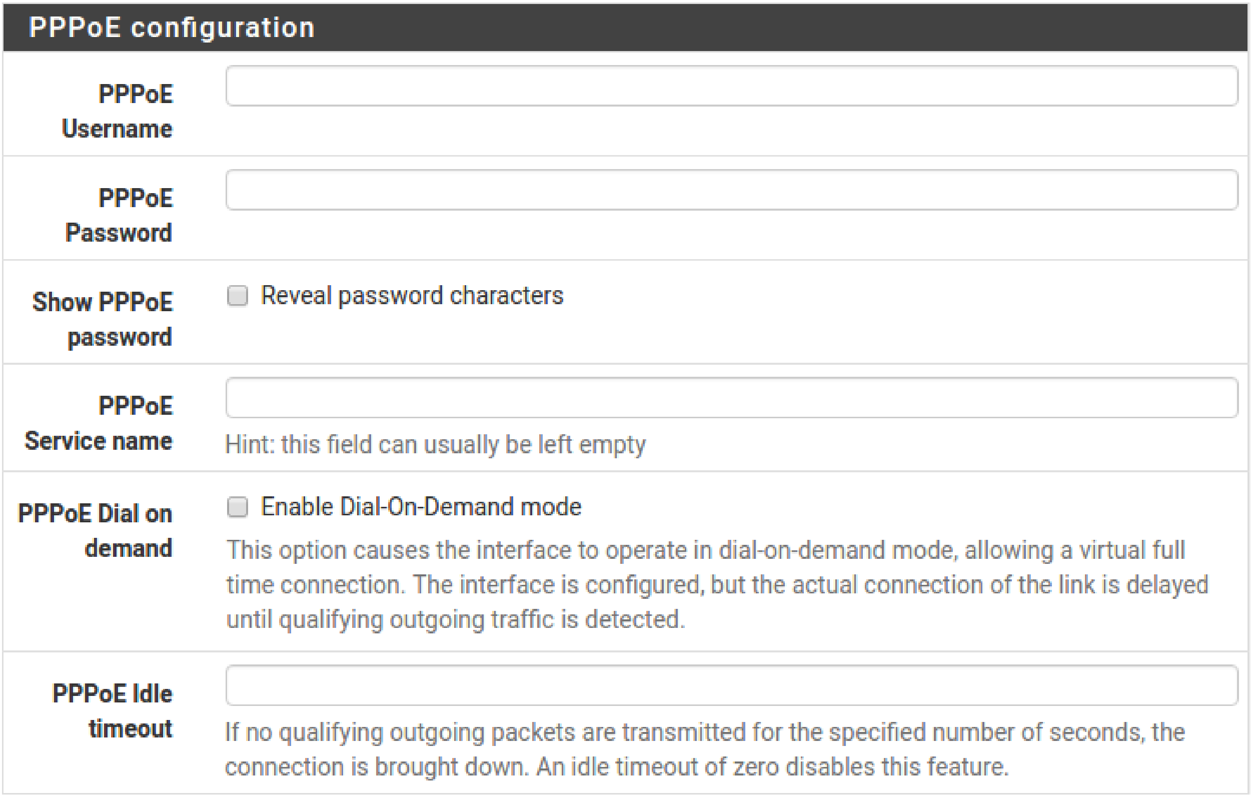


DHCP client configuration

DHCP Hostname	The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

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

1.1.15 Configuring PPPoE and PPTP Interfaces

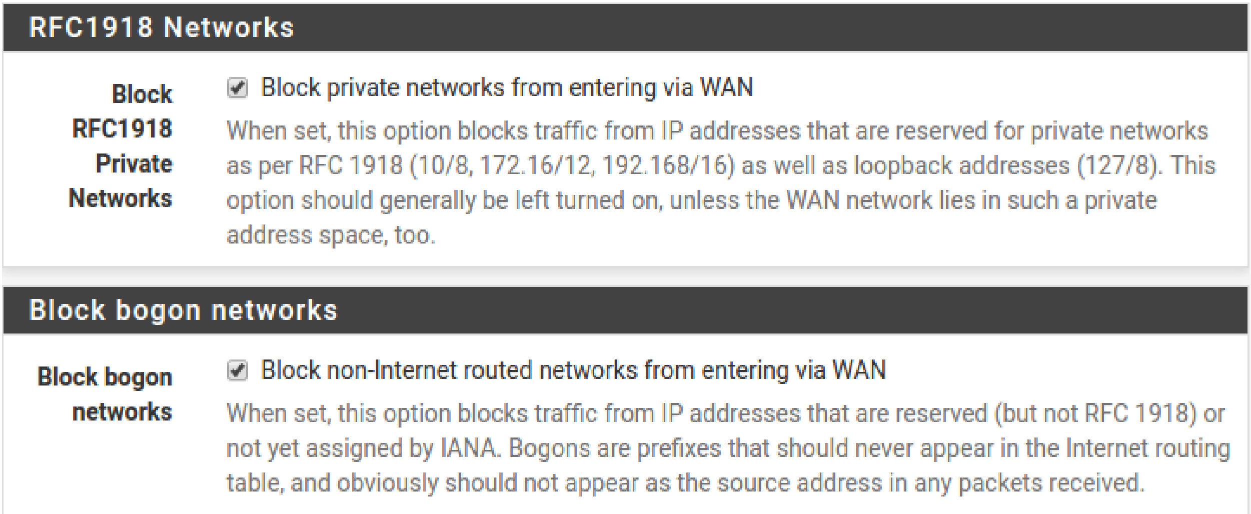


PPPoE configuration

PPPoE Username	
PPPoE Password	
Show PPPoE password	□ Reveal password characters
PPPoE Service name	Hint: this field can usually be left empty
PPPoE Dial on demand	□ Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPPoE Idle timeout	If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

Information added in these sections is assigned by the ISP. Configure these settings as directed by the ISP

1.1.16 Block Private Networks and Bogons



RFC1918 Networks

Block RFC1918 Private Networks ☑ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks ☑ Block non-Internet routed networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

When enabled, the firewall will block all private network traffic from entering the WAN interface.

Private addresses are reserved for use on internal LANs and blocked from outside traffic so these address ranges may be reused by all private networks.

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

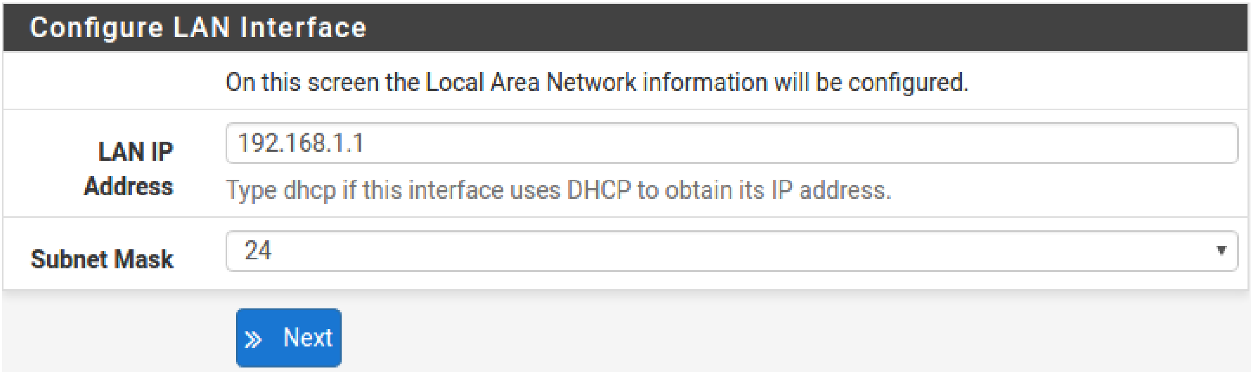
- `10.0.0.1` to `10.255.255.255`
- `172.16.0.1` to `172.31.255.254`
- `192.168.0.1` to `192.168.255.254`
- `127.0.0.0/8`
- `100.64.0.0/10`
- `fc00::/7`

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

Check **Block RFC1918 Private Networks** and **Block Bogon Networks**.

Click **Next** to continue.

1.1.17 Configuring LAN IP Address & Subnet Mask



Configure LAN Interface

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

LAN IP Address 192.168.1.1

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask 24

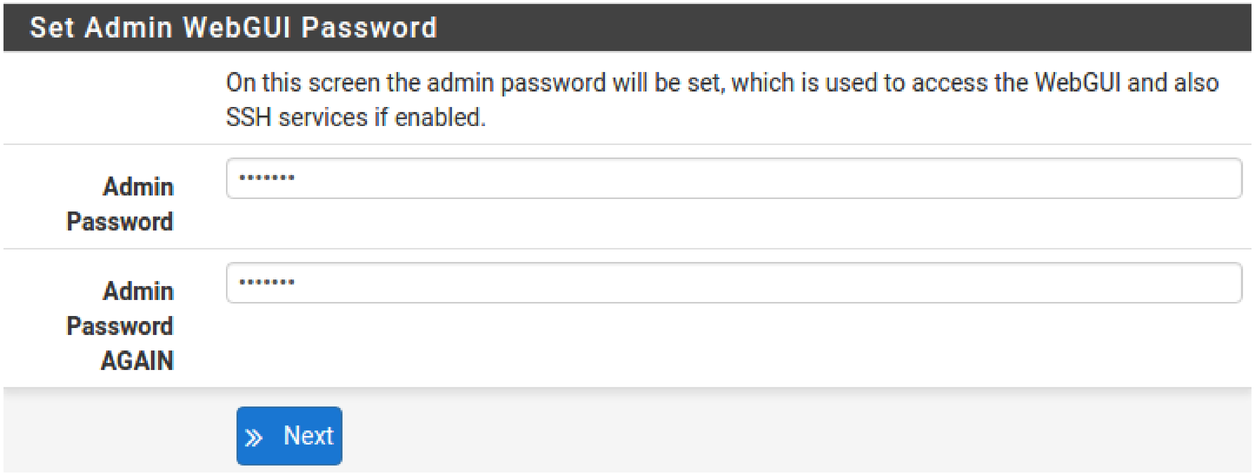
A static IP address of `192.168.1.1` and a subnet mask (CIDR) of `24` was chosen for this installation. If there are no plans to connect this network to any other network via VPN, the `192.168.1.x` default is sufficient.

Click **Next** to continue.

Note: If a Virtual Private Network (VPN) is configured to remote locations, choose a private IP address range more obscure than the very common `192.168.1.0/24`. IP addresses within the `172.16.0.0/12` RFC1918 private address block are the least frequently used.

The best practice is to select a block of addresses between `172.16.x.x` and `172.31.x.x` for least likelihood of having VPN connectivity difficulties. An example of a conflict would be If the local LAN is set to `192.168.1.x` and a remote user is connected to a wireless hotspot using `192.168.1.x` (very common), the remote client won't be able to communicate across the VPN to the local network.

1.1.18 Change Administrator Password



Set Admin WebGUI Password

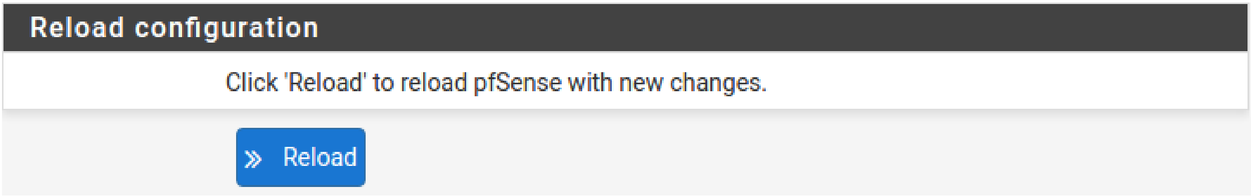
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: •••••••

Admin Password AGAIN: •••••••

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

1.1.19 Save Changes

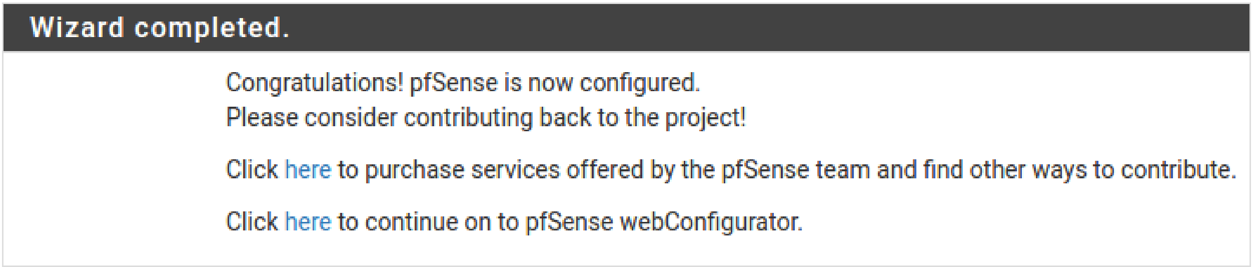


Reload configuration

Click 'Reload' to reload pfSense with new changes.

Click **Reload** to save configuration.

1.1.20 Basic Firewall Configured



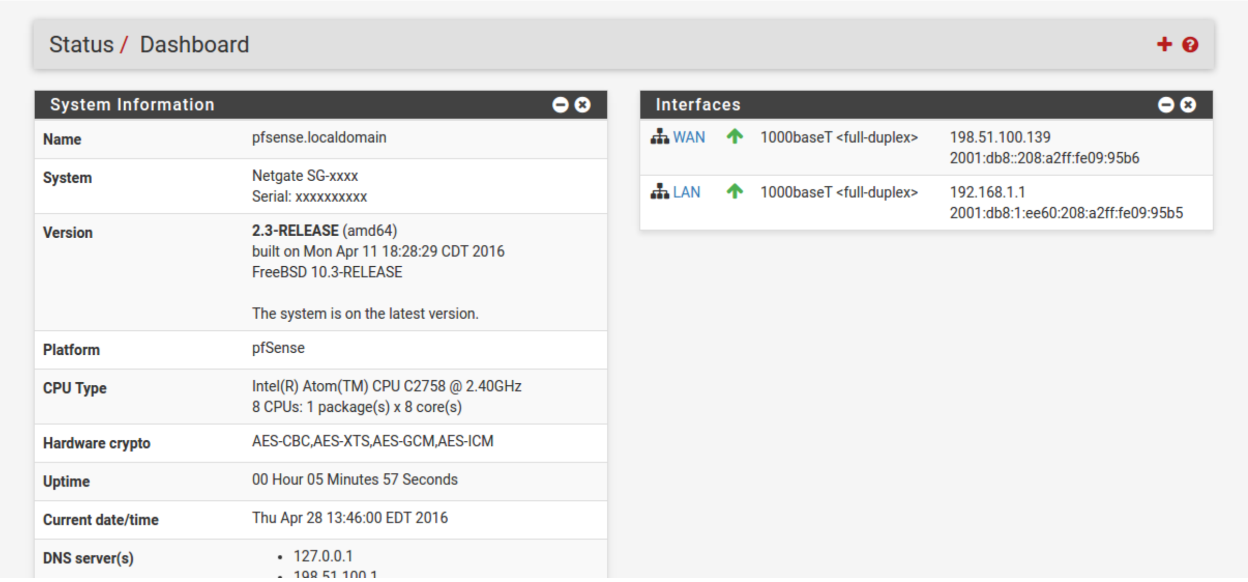
Wizard completed.

Congratulations! pfSense is now configured.
Please consider contributing back to the project!

Click here to purchase services offered by the pfSense team and find other ways to contribute.

Click here to continue on to pfSense webConfigurator.

To proceed to the GUI, make the selection as highlighted. The browser will then display the Dashboard.



Status / Dashboard

System Information

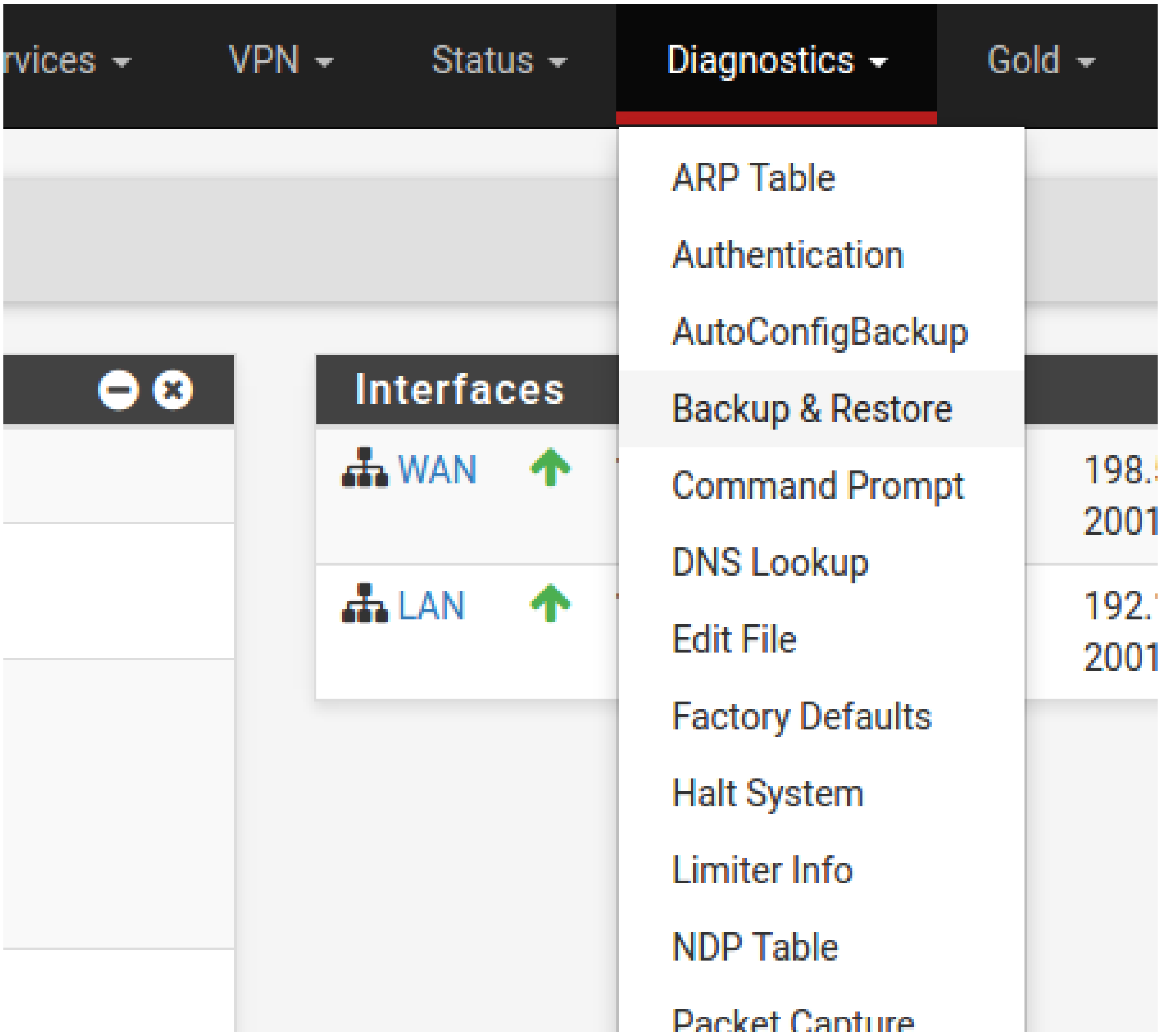
Name	pfsense.localdomain
System	Netgate SG-xxxx Serial: xxxxxxxxxx
Version	**2.3-RELEASE** (amd64) built on Mon Apr 11 18:28:29 CDT 2016 FreeBSD 10.3-RELEASE The system is on the latest version.
Platform	pfSense
CPU Type	Intel(R) Atom(TM) CPU C2758 @ 2.40GHz 8 CPUs: 1 package(s) x 8 core(s)
Hardware crypto	AES-CBC,AES-XTS,AES-GCM,AES-ICM
Uptime	00 Hour 05 Minutes 57 Seconds
Current date/time	Thu Apr 28 13:46:00 EDT 2016
DNS server(s)	• 127.0.0.1 • 198.51.100.1

Interfaces

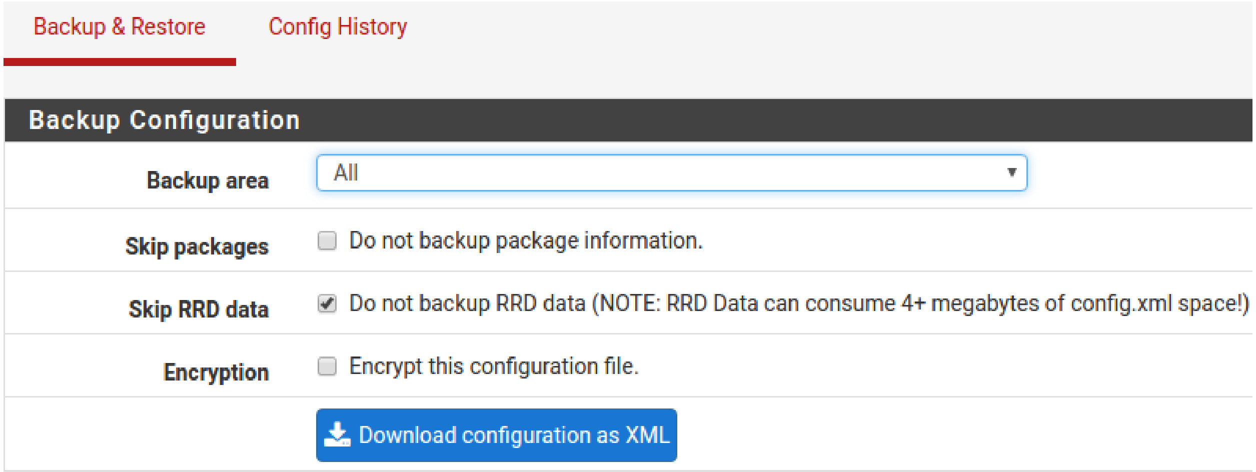
WAN	1000baseT <full-duplex>	198.51.100.139 2001:db8::208:a2ff:fe09:95b6
LAN	1000baseT <full-duplex>	192.168.1.1 2001:db8:1:ee60:208:a2ff:fe09:95b5

1.1.21 Backing Up and Restoring

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



Click **Download Configuration** and save a copy of the firewall configuration.



Backup Configuration

Backup area	All
Skip packages	☐ Do not backup package information.
Skip RRD data	☑ Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)
Encryption	☐ Encrypt this configuration file.

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

1.1.22 Connecting to the Console

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

See also:

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

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

1.2 Initial Configuration

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

Warning: If the CPE on WAN (e.g. Fiber or Cable Modem) has a default IP Address of `192.168.1.1`, disconnect the Ethernet cable from the WAN port on the Netgate 1537 1U 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`.

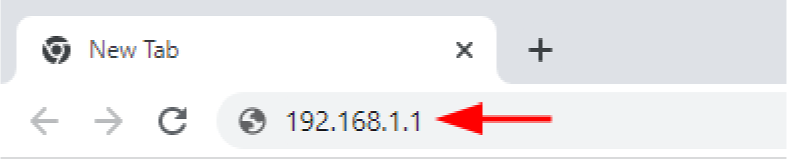
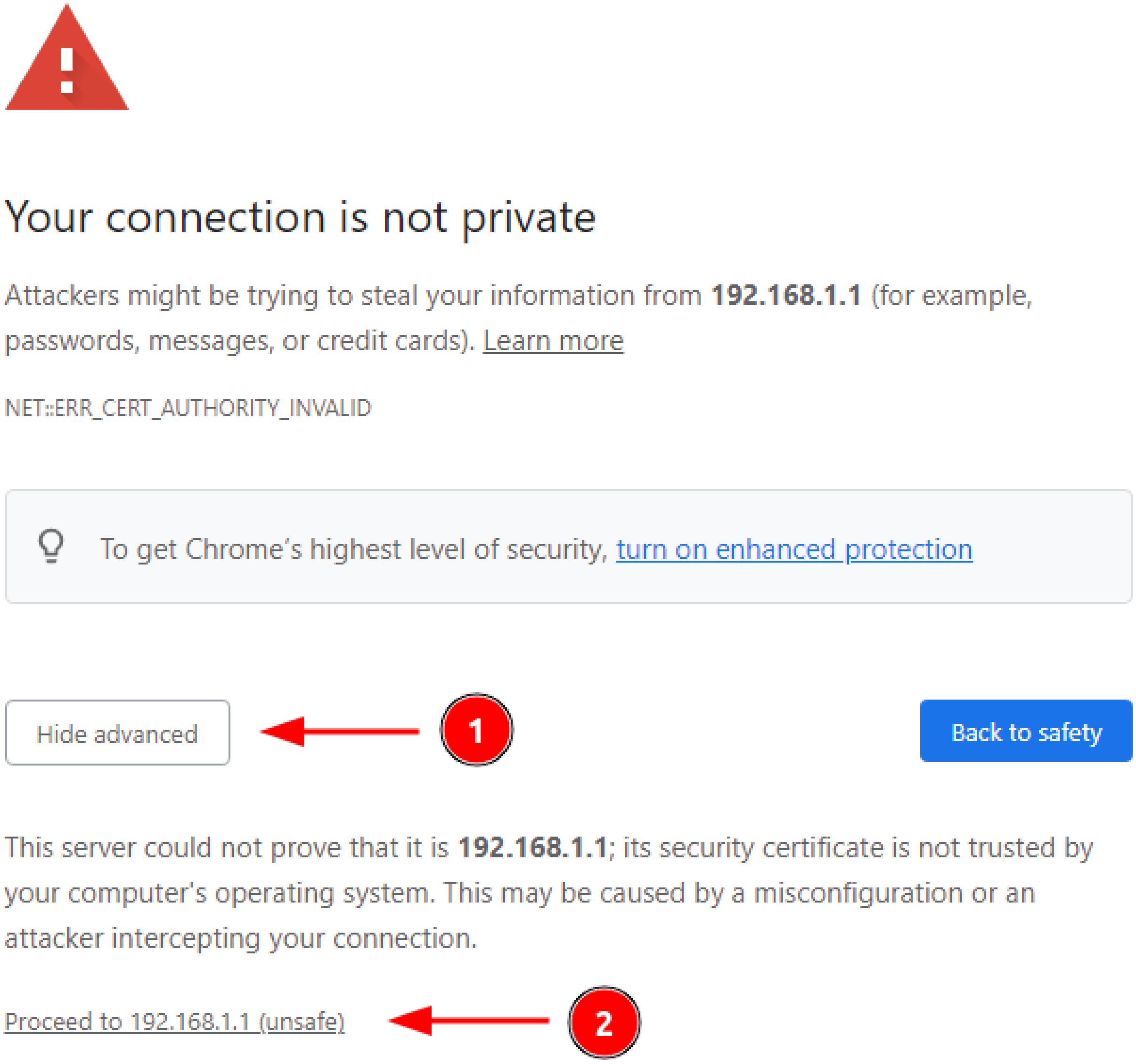


Fig. 1: Enter the default LAN IP address in the browser

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`



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

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.

Fig. 2: Example certificate warning message

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.

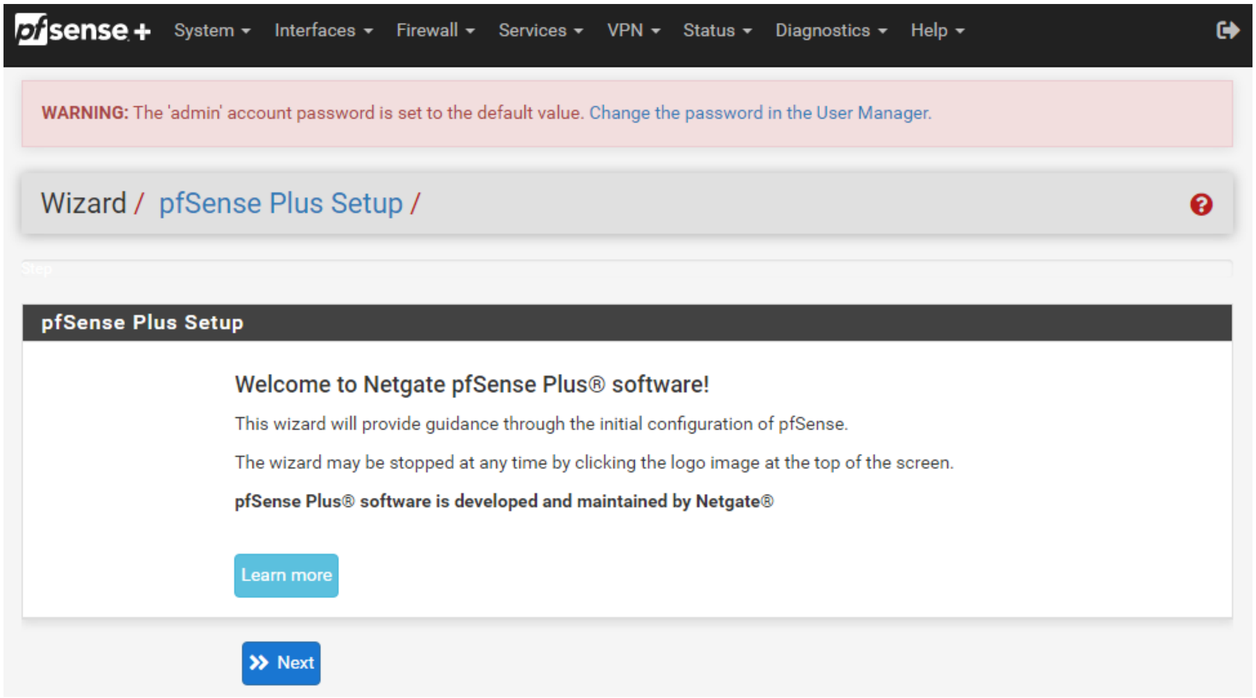
Tip: The wizard can be safely stopped at any time for those who wish to perform the configuration manually or restore an existing backup (Backup and Restore).

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.

---

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



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Plus Setup /

pfSense Plus Setup

Welcome to Netgate pfSense Plus® software!

This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

pfSense Plus® software is developed and maintained by Netgate®

Fig. 3: Setup Wizard starting page

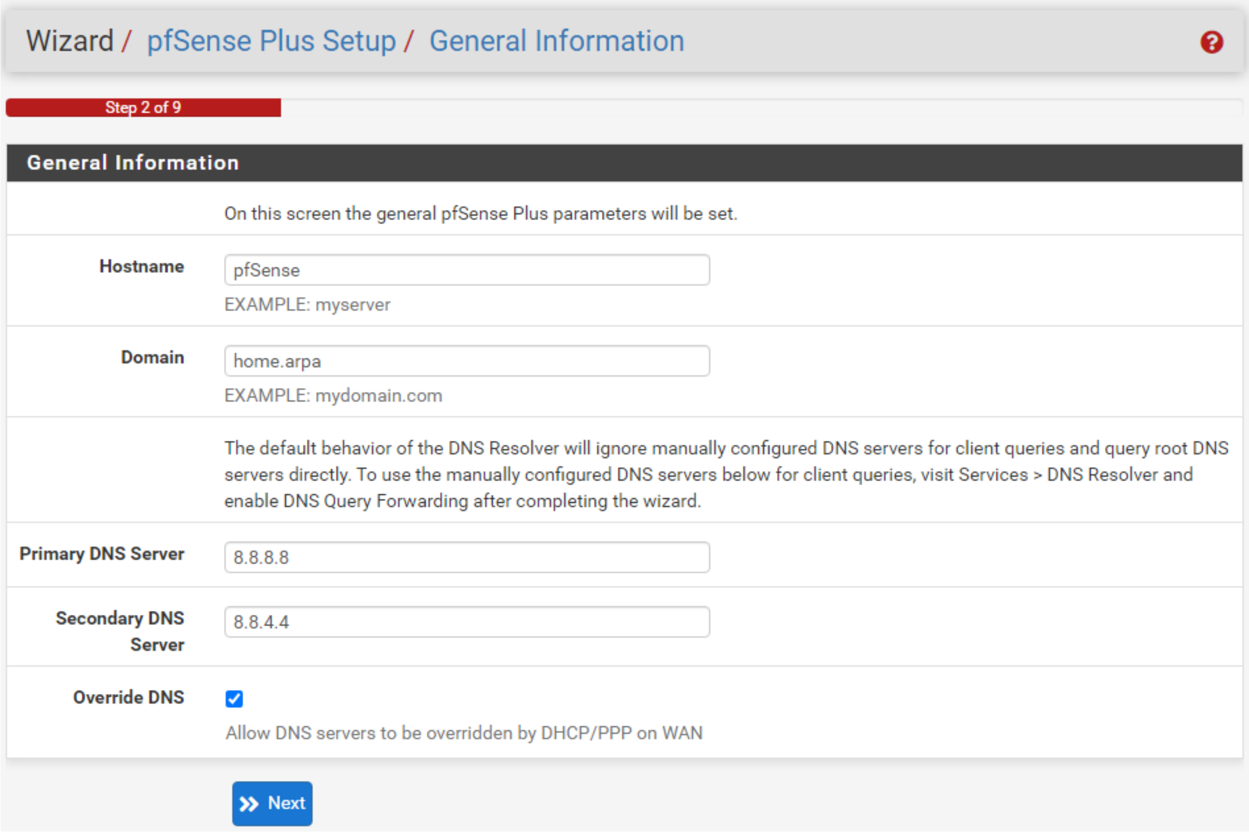
2. Click **Next** after reading the information on **Netgate Global Support**.
3. Use the following items as a guide to configure the options on the **General Information** page:

   Hostname Any desired hostname name can be entered to identify the firewall. For the purposes of this guide, the default hostname `pfsense` is used.

   Domain The domain name under which the firewall operates. The default `home.arpa` is used for the purposes of this tutorial.

DNS Servers For purposes of this setup guide, use the Google public DNS servers (`8.8.8.8` and `8.8.4.4`).

> **Note:** The firewall defaults to acting as a resolver and clients will not utilize these forwarding DNS servers. However, these servers give the firewall itself a way to ensure it has working DNS if resolving the default way does not work properly.



Wizard / pfSense Plus Setup / General Information

Step 2 of 9

General Information

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

Hostname	pfSense EXAMPLE: myserver
Domain	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	8.8.8.8
Secondary DNS Server	8.8.4.4
Override DNS	☑ Allow DNS servers to be overridden by DHCP/PPP on WAN

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

Type in the DNS Server information and Click **Next**.

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

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

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

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

   Change the Timezone and click **Next**.

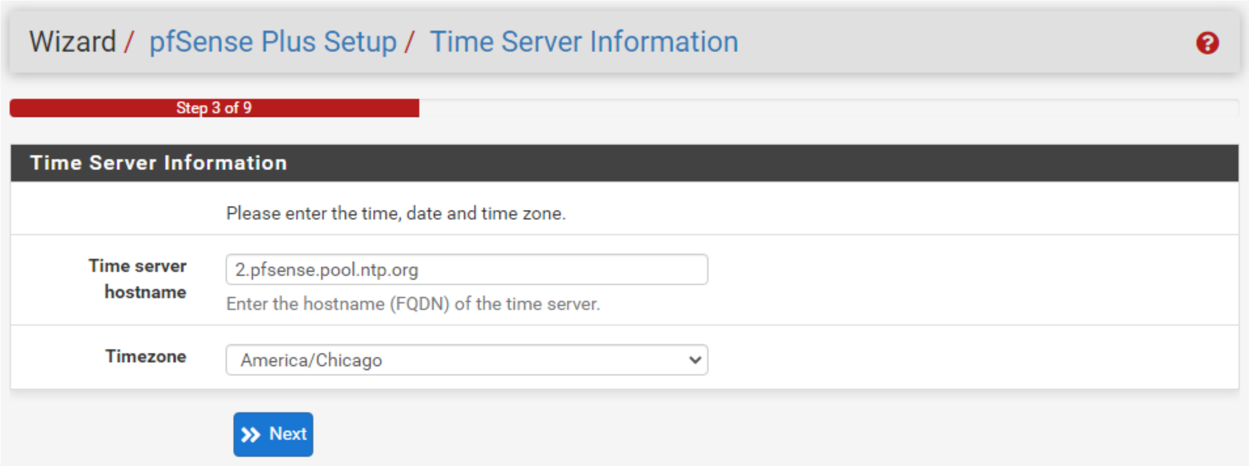
5. Use the following information for the **Configure WAN Interface** page:

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

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

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

   Default settings should be acceptable. Click **Next**.



Wizard / pfSense Plus Setup / Time Server Information

Step 3 of 9

Time Server Information

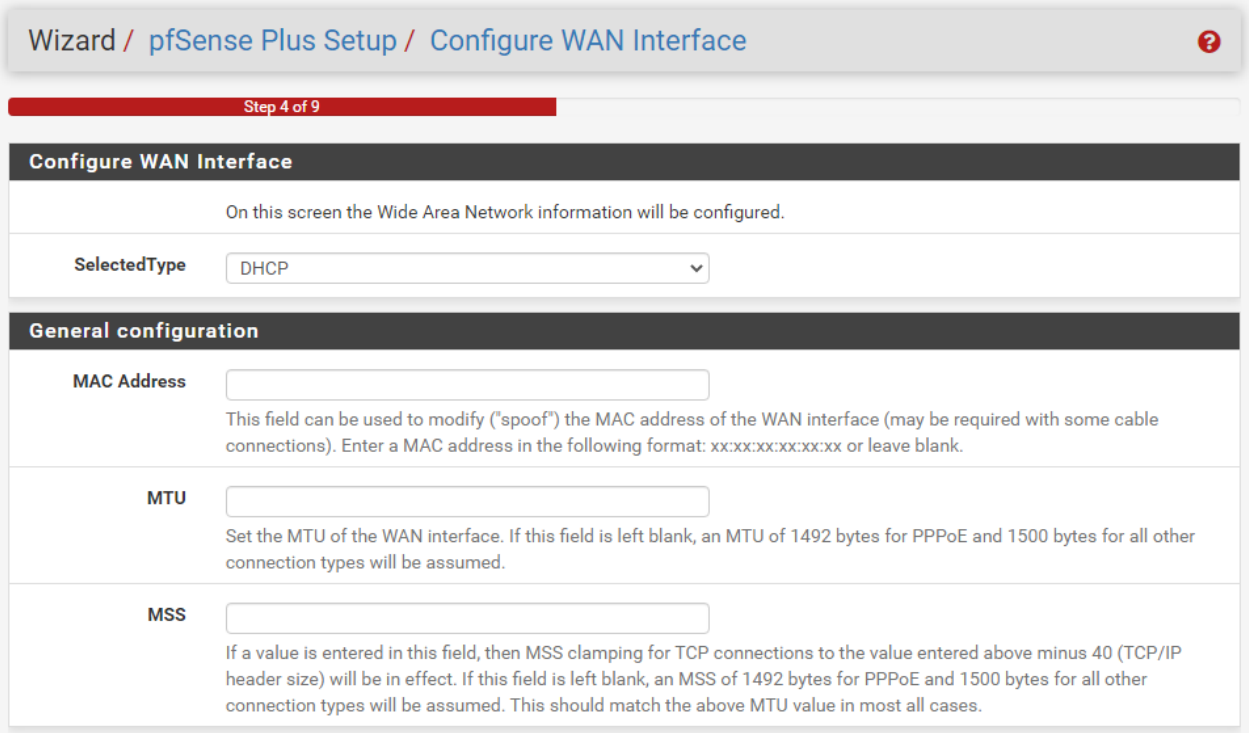
Please enter the time, date and time zone.

Time server hostname: 2.pfsense.pool.ntp.org

Enter the hostname (FQDN) of the time server.

Timezone: America/Chicago

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

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 WAN port on the Netgate 1537 1U 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.

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 WAN port now.

This completes the basic configuration for the Netgate appliance.

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

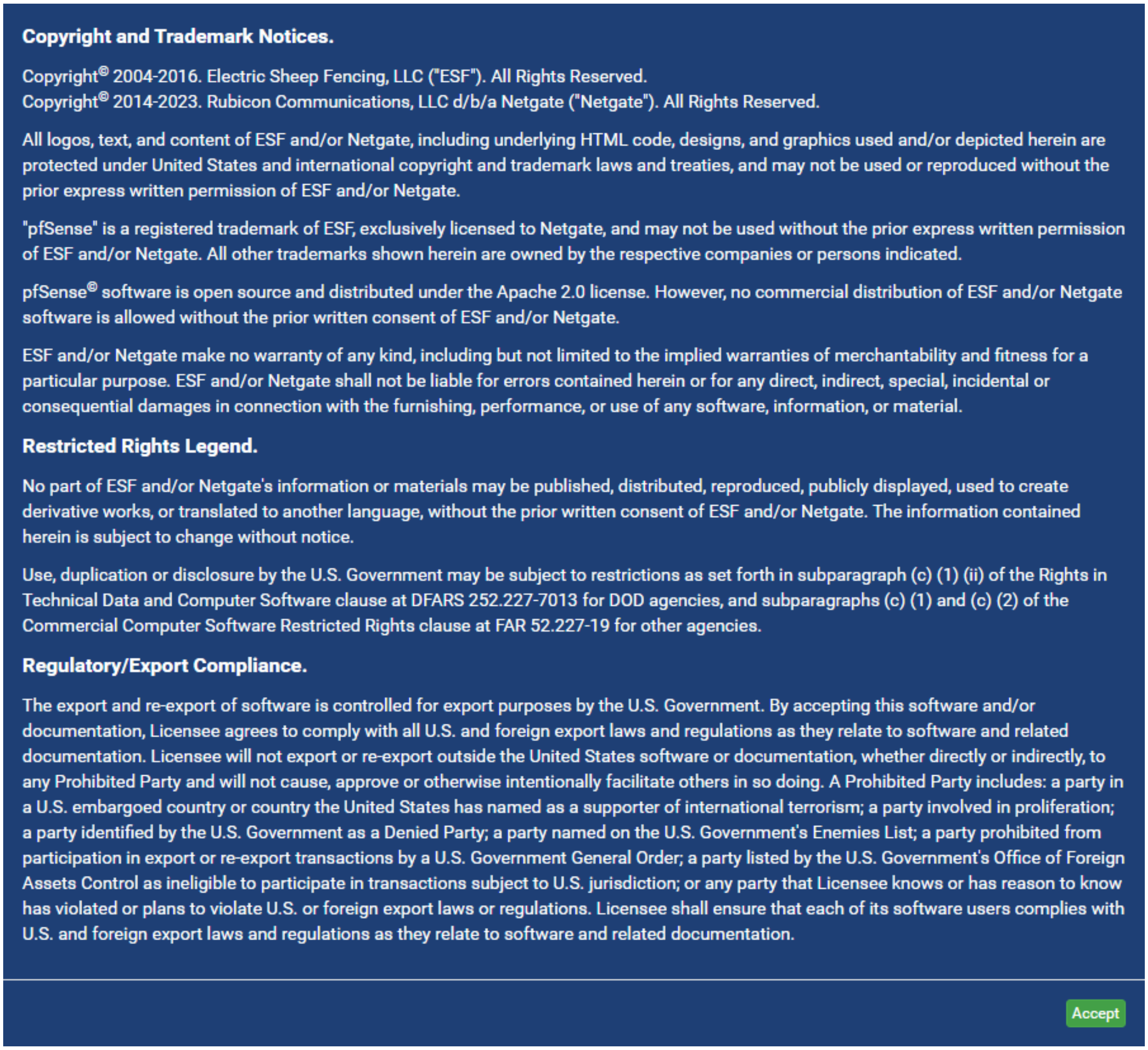
pfSense® Plus software is highly configurable, all of which can be done through the dashboard. This orientation will help to navigate and further configure the firewall.

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.



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.

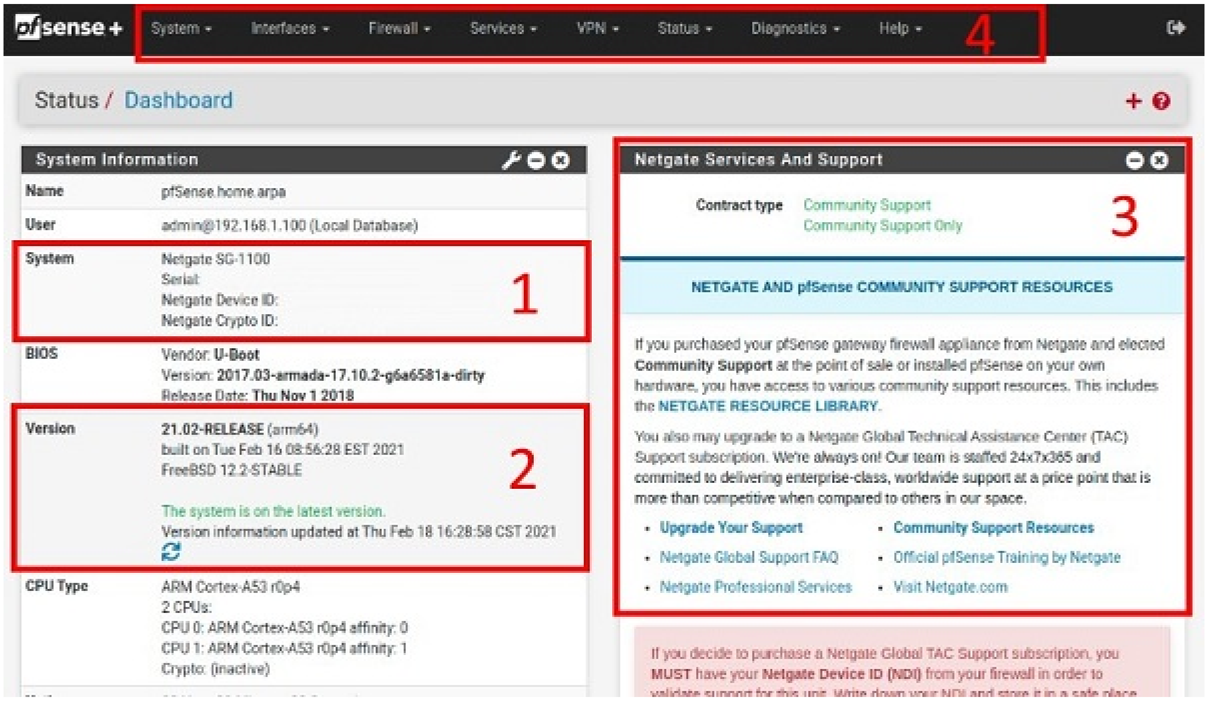
No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without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

Fig. 7: Copyright and Trademark Notices



Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.1.100 (Local Database)
System	Netgate SG-1100 Serial: Netgate Device ID: Netgate Crypto ID:
BIOS	Vendor: **U-Boot** Version: **2017.03-armada-17.10.2-g6a6581a-dirty** Release Date: **Thu Nov 1 2018**
Version	**21.02-RELEASE** (arm64) built on Tue Feb 16 08:56:28 EST 2021 FreeBSD 12.2-STABLE The system is on the latest version. Version information updated at Thu Feb 18 16:28:58 CST 2021
CPU Type	ARM Cortex-A53 r0p4 2 CPUs: CPU 0: ARM Cortex-A53 r0p4 affinity: 0 CPU 1: ARM Cortex-A53 r0p4 affinity: 1 Crypto: (inactive)

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- **Upgrade Your Support**
- Netgate Global Support FAQ
- Netgate Professional Services
- **Community Support Resources**
- Official pfSense Training by Netgate
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place.

Fig. 8: The pfSense® Plus Dashboard

1.3.2 Re-running the Setup Wizard

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

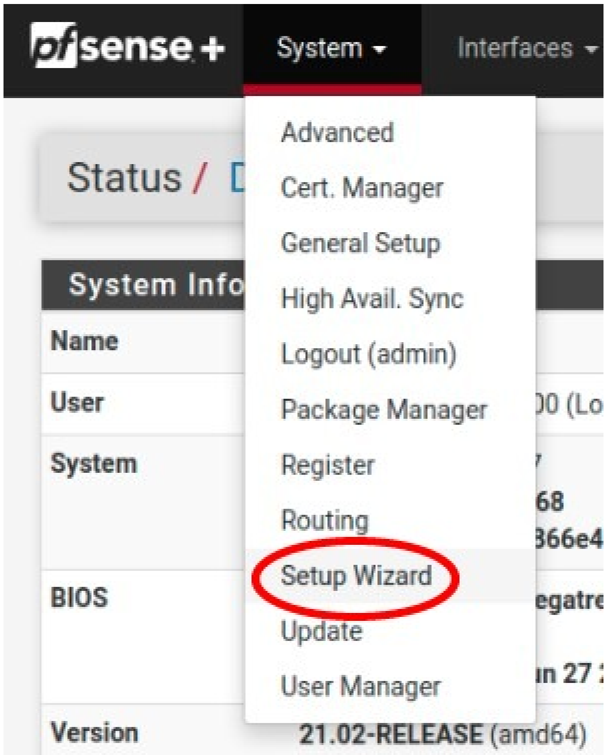


Fig. 9: Re-run the Setup Wizard

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 peform a manual check as well by visiting **System > Update**.

Users can initiate an upgrade from the **System > Update** page as needed.

For more information, see the Upgrade Guide.

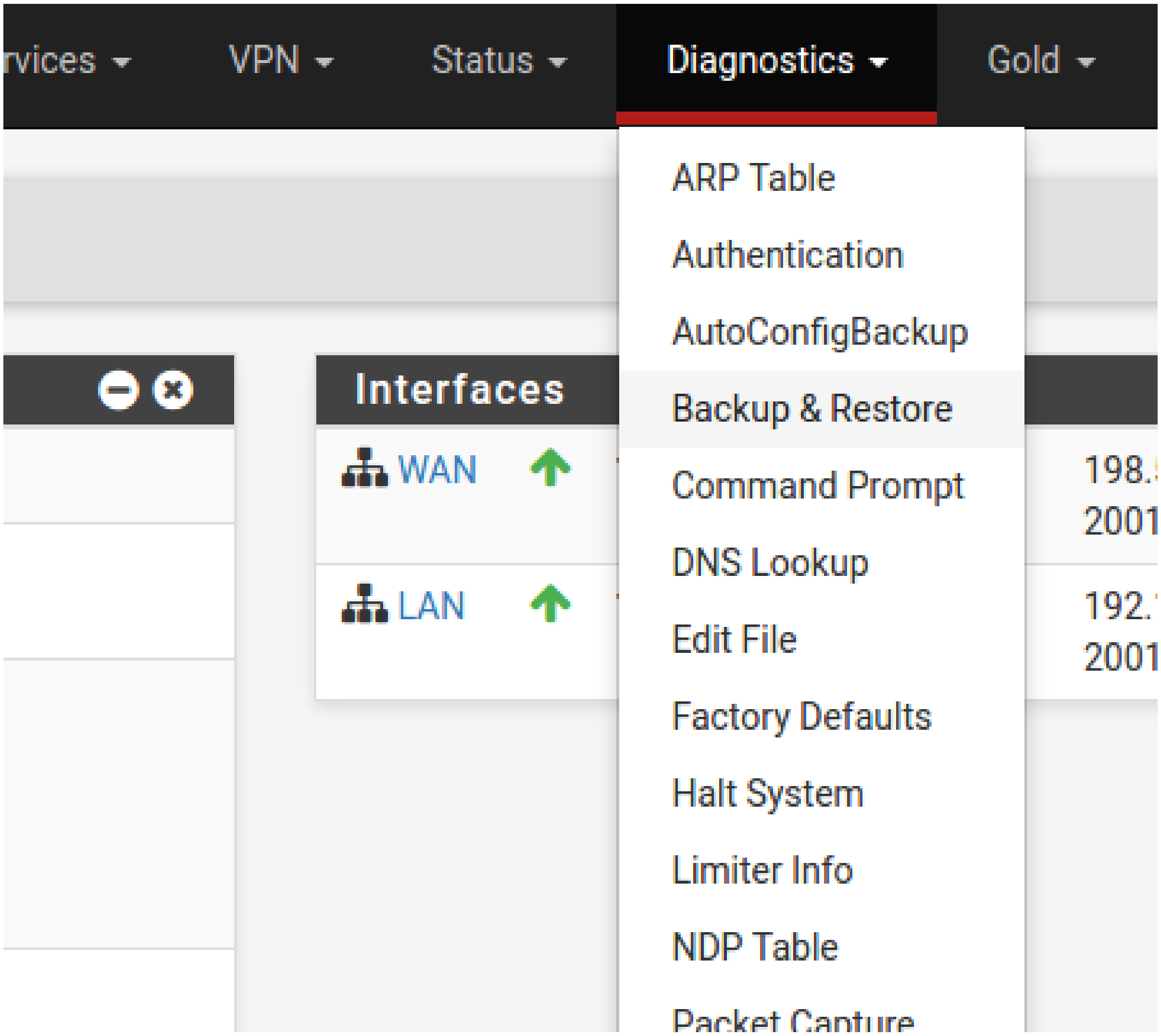
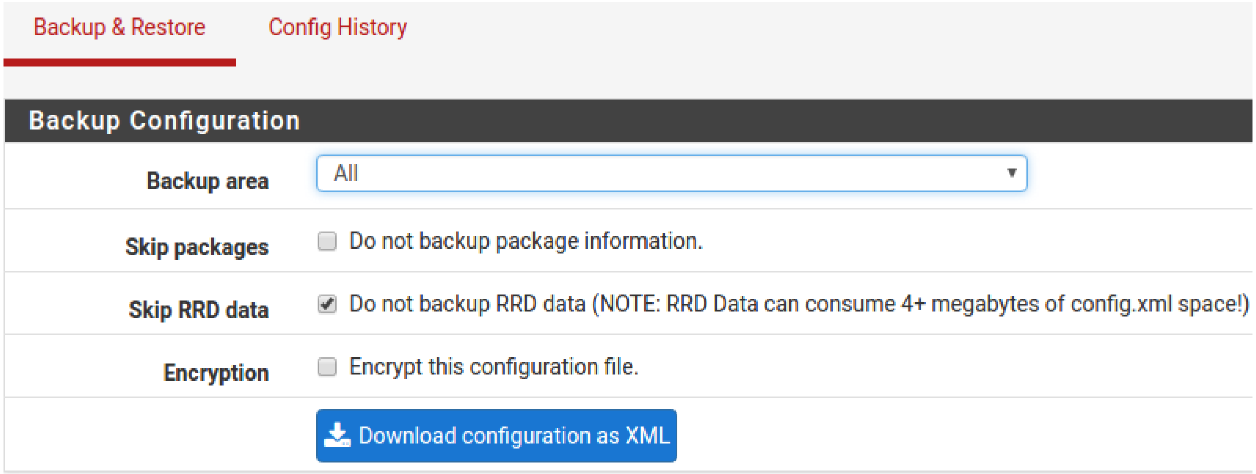


Fig. 10: Backup & Restore



Backup & Restore | Config History

Backup Configuration

Backup area	All
Skip packages	□ Do not backup package information.
Skip RRD data	☑ Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)
Encryption	□ Encrypt this configuration file.

Download configuration as XML

Fig. 11: Click Download configuration as XML

1.4 Input and Output Ports

1.4.1 Front Side

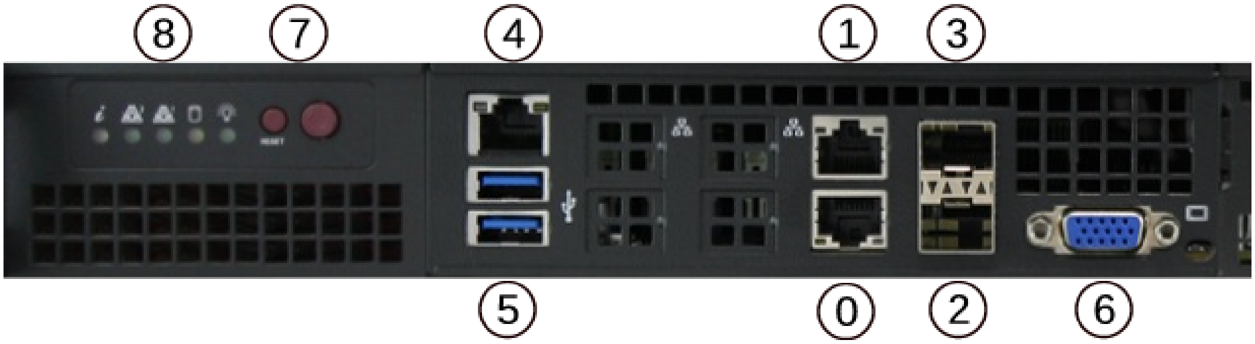


Fig. 12: Front view of the Netgate 1537 Firewall Appliance
The numbered labels in this image refer to entries in *Network Ports* and *Other Ports*.

Network Ports

Default Ports

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

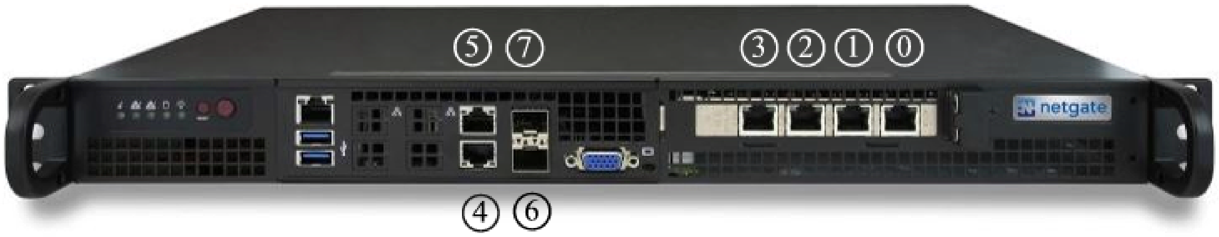
Port	Interface Name	Port Name	Port Type	Port Speed
0	WAN	igb0	RJ-45	1 Gbps
1	LAN	igb1	RJ-45	1 Gbps
2	OPT1	ix0	SFP+	10 Gbps
3	OPT2	ix1	SFP+	10 Gbps

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

Optional Quad Port Expansion Cards

Default port configuration for 4-port expansion cards.

- 4-port 1GbE Supermicro AOC-SGP-i4
- 4-port 10GbE Intel X710BM2

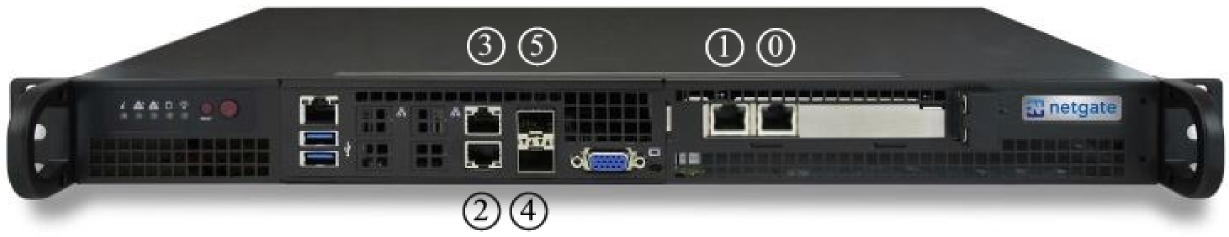


Port	Interface Name		Port Name		Port Type		Port Speed	
#	SGP-i4	X710	SGP-i4	X710	SGP-i4	X710	SGP-i4	X710
0	OPT6	Unassigned	igb0	ixl0	RJ-45	SFP+	1 Gbps	10 Gbps
1	OPT5	Unassigned	igb1	ixl1	RJ-45	SFP+	1 Gbps	10 Gbps
2	OPT4	Unassigned	igb2	ixl2	RJ-45	SFP+	1 Gbps	10 Gbps
3	OPT3	Unassigned	igb3	ixl3	RJ-45	SFP+	1 Gbps	10 Gbps
4	WAN	WAN	igb4	igb0	RJ-45	RJ-45	1 Gbps	1 Gbps
5	LAN	LAN	igb5	igb1	RJ-45	RJ-45	1 Gbps	1 Gbps
6	OPT1	OPT1	ix0	ix0	SFP+	SFP+	10 Gbps	10 Gbps
7	OPT2	OPT2	ix1	ix1	SFP+	SFP+	10 Gbps	10 Gbps

Optional Dual Port Expansion Cards

Default port configuraiton for 2-port expansion cards.

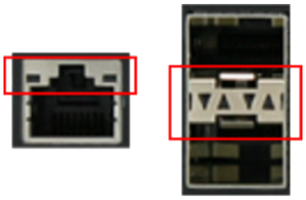
- 2-port 10GbE Chelsio T520-CR
- 2-port 10GbE Intel X710BM2



Port	Interface Name		Port Name		Port Type	Port Speed
#	T520	X710	T520	X710	T520/X710	T520/X710
0	WAN	Unassigned	cxl0	ixl0	SFP+	10 Gbps
1	LAN	Unassigned	cxl1	ixl1	SFP+	10 Gbps
2	OPT1	WAN	igb0	igb0	RJ-45	1 Gbps
3	OPT3	LAN	igb1	igb1	RJ-45	1 Gbps
4	OPT2	OPT1	ix0	ix0	SFP+	10 Gbps
5	OPT4	OPT2	ix1	ix1	SFP+	10 Gbps

Network Port LEDs

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



RJ-45 Ports

Table 1: RJ-45 LEDs Configuration

Activity LED (Left)	Link Speed LED (Right)

Off = No Connection
Yellow Flashing = Activity
	Amber = 1 Gbps
	Green = 100 Mbps
	Off = No Connection or 10 Mbps

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

SFP+ Ports

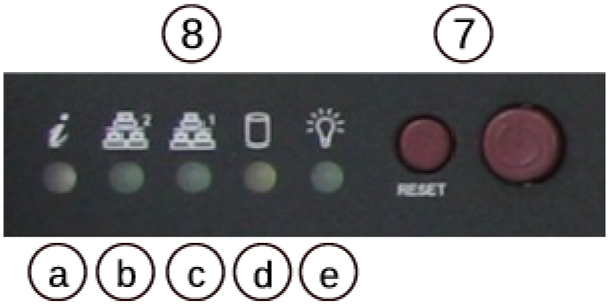
Table 2: SFP+ LEDs Configuration

Left Two LEDs	Right Two LEDs

Off = No Connection
Green = Connection Established
	Green Blinking = Activity

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

Status LEDs



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

Other Ports

Port	I/O Type
4	IPMI
5	2x USB 3.0 Ports
6	*VGA Console*
7	Reset & Power buttons
8	Status LEDs

USB Ports

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

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

1.4.2 Rear Side

Other Ports

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

1.5 Safety and Legal

1.5.1 Safety Notices

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

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

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

1.5.2 Electrical Safety Information

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

Warning: To help protect your Netgate appliance from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, uninterruptible power supply (UPS) or a combination of those devices.

Failure to take such precautions could result in premature failure, and/or damage to your Netgate appliance, which is not covered under the product warranty. Such an event may also present the risk of electric shock, fire, or explosion.

1.5.3 FCC Compliance

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

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

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

1.5.4 Industry Canada

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

1.5.5 Australia and New Zealand

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

1.5.6 CE Marking

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

1.5.7 RoHS/WEEE Compliance Statement

English

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

Deutsch

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

Español

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

Français

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

Italiano

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

1.5.8 Declaration of Conformity

Česky[Czech]

NETGATE tímto prohla uje, e tento NETGATE device, je ve shod se základními po adavky a dal ími p íslu n mi ustanoveními sm rnice 1999/5/ES.

Dansk [Danish]

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

Nederlands [Dutch]

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

English

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

Eesti [Estonian]

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

Suomi [Finnish]

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

Deutsch [German]

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

ΕλληνιxΗ [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 alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.

Íslenska [Icelandic]

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

Italiano [Italian]

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

Latviski [Latvian]

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

Lietuviškai [Lithuanian]

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

Malti [Maltese]

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

Norsk [Norwegian]

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

Slovensky [Slovak]

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

Svenska [Swedish]

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

Español [Spanish]

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

Polski [Polish]

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

Português [Portuguese]

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

Română [Romanian]

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

1.5.9 Disputes

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

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

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

Rubicon Communications LLC
Attn.: Legal Dept.
4616 West Howard Lane, Suite 900
Austin, Texas 78728
legal@netgate.com

The arbitration will be conducted by the American Arbitration Association (AAA) under its rules. The AAA's rules are available at www.adr.org. Payment of all filing, administration and arbitrator fees will be governed by the AAA's rules.

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

1.5.10 Applicable Law

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

1.5.11 Site Policies, Modification, and Severability

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

1.5.12 Miscellaneous

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

1.5.13 Limited Warranty

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

THE PRODUCTS/SERVICES AND ALL INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOFTWARE) AND OTHER SERVICES INCLUDED ON OR OTHERWISE MADE AVAILABLE TO YOU THROUGH THE PRODUCTS/SERVICES ARE PROVIDED BY US ON AN “AS IS” AND “AS AVAILABLE” BASIS, UNLESS OTHERWISE SPECIFIED IN WRITING. WE MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE OPERATION OF THE PRODUCTS/SERVICES, OR THE INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOFTWARE) OR OTHER SERVICES INCLUDED ON OR OTHERWISE MADE AVAILABLE TO YOU THROUGH THE PRODUCTS/SERVICES, UNLESS OTHERWISE SPECIFIED IN WRITING. YOU EXPRESSLY AGREE THAT YOUR USE OF THE PRODUCTS/SERVICES IS AT YOUR SOLE RISK.

TO THE FULL EXTENT PERMISSIBLE BY APPLICABLE LAW, RUBICON COMMUNICATIONS, LLC (RCL) AND ELECTRIC SHEEP FENCING (ESF) DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. RCL AND ESF DO NOT WARRANT THAT THE PRODUCTS/SERVICES, INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOFTWARE) OR OTHER SERVICES INCLUDED ON OR OTHERWISE MADE AVAILABLE TO YOU THROUGH THE PRODUCTS/SERVICES, RCL’S OR ESF’S SERVERS OR ELECTRONIC COMMUNICATIONS SENT FROM RCL OR ESF ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS. RCL AND ESF WILL NOT BE LIABLE FOR ANY DAMAGES OF ANY KIND ARISING FROM THE USE OF ANY PRODUCTS/SERVICES, OR FROM ANY INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOFTWARE) OR OTHER SERVICES INCLUDED ON OR OTHERWISE MADE AVAILABLE TO YOU THROUGH ANY PRODUCTS/SERVICES, INCLUDING, BUT NOT LIMITED TO DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, AND CONSEQUENTIAL DAMAGES, UNLESS OTHERWISE SPECIFIED IN WRITING.

IN NO EVENT WILL RCL’S OR ESF’S LIABILITY TO YOU EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT OR SERVICE THAT IS THE BASIS OF THE CLAIM.

CERTAIN STATE LAWS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES OR THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES. IF THESE LAWS APPLY TO YOU, SOME OR ALL OF THE ABOVE DISCLAIMERS, EXCLUSIONS, OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MIGHT HAVE ADDITIONAL RIGHTS.

CHAPTER

TWO

HOW-TO GUIDES

2.1 Connecting to the Console Port

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

Note: If the device has both USB 2.0 (black) and USB 3.0 (blue) ports, use the USB 2.0 ports for better compatibility.

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

2.2 Accessing IPMI and Changing IPMI Password

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

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

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

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

Note: The password is alpha-numeric and the letters are capital letters.

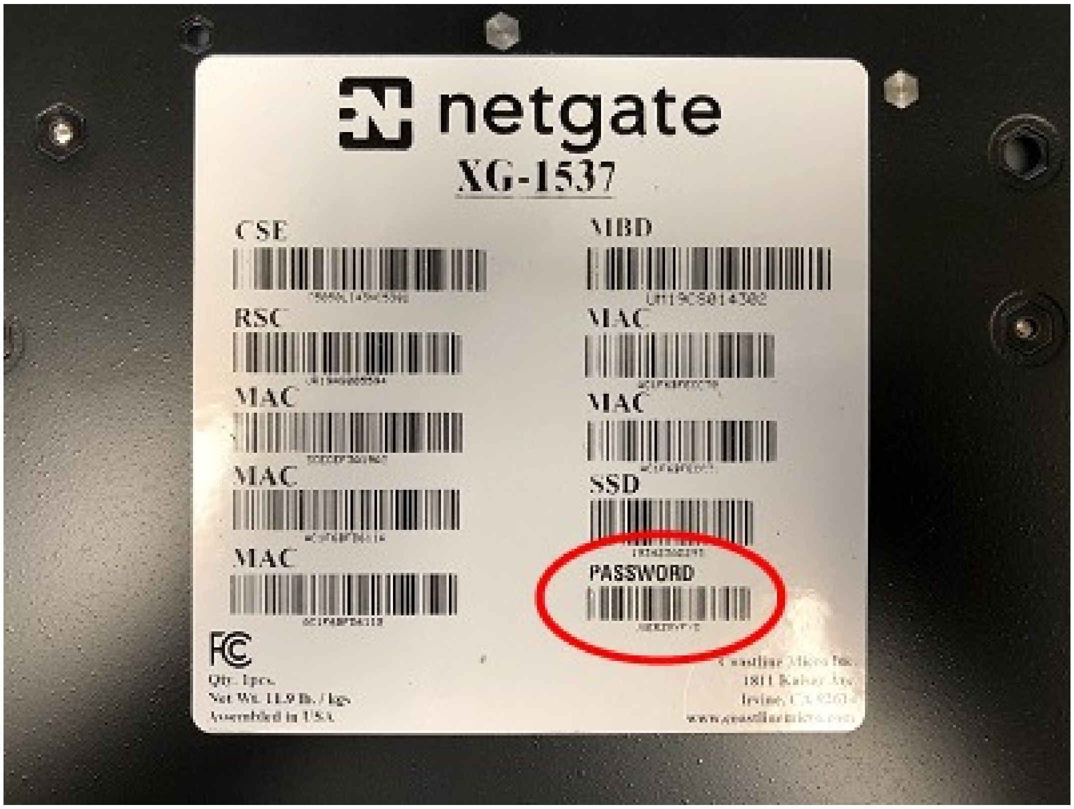


Fig. 1: IPMI Password Sticker Location

2.3 Changing the IPMI Password

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

2.3.1 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

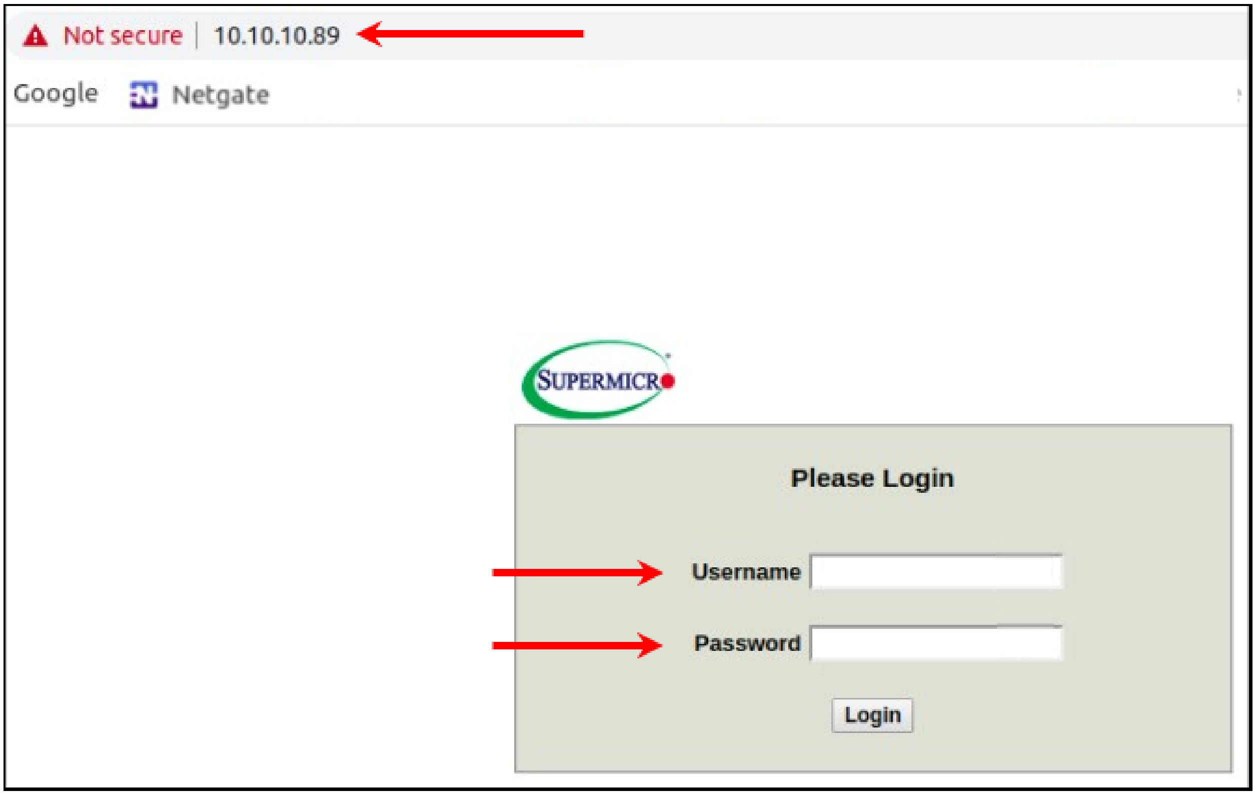


Fig. 2: Log Into IPMI

- Navigate to **Configuration > Users**
- Select the user to modify

  This is likely the `ADMIN` user or another user with *Administrator* privileges.
- Click **Modify User**
- Check **Change Password**
- Enter the new **Password**
- Enter it again in **Confirm Password**
- Click **Modify**
- Click **OK** on the message window that says "Modified user successfully."

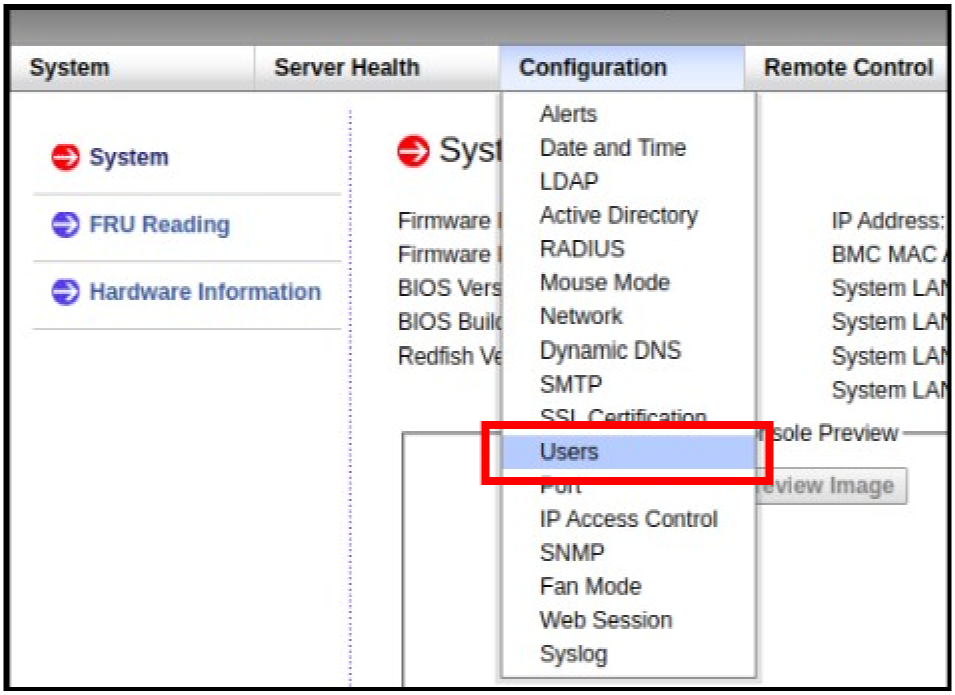
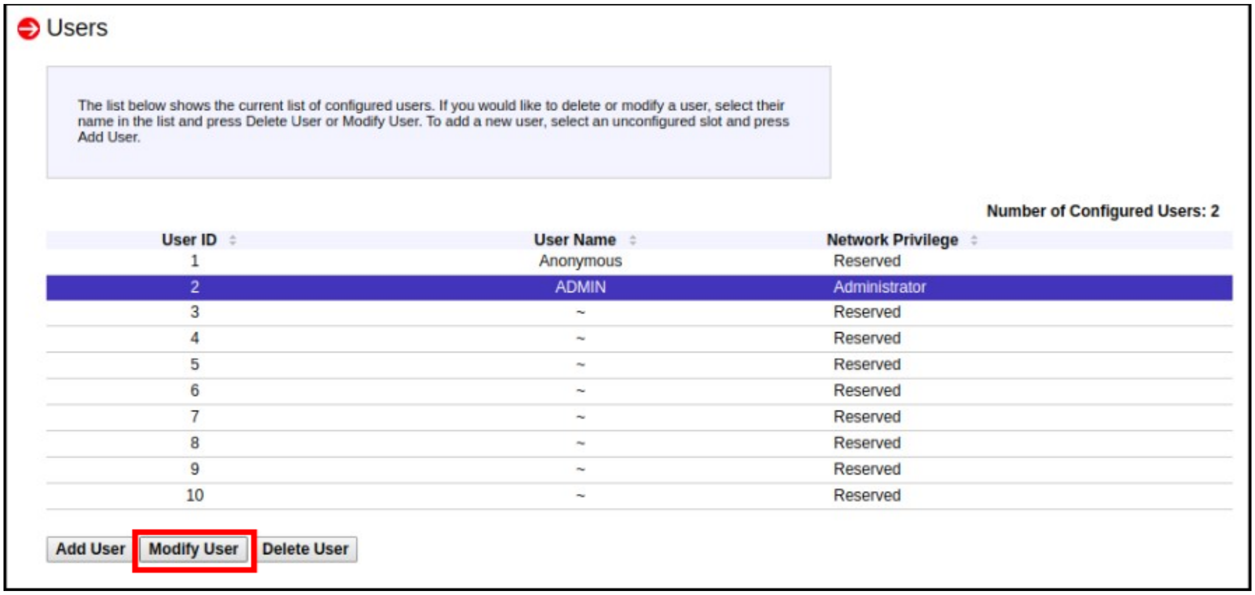


Fig. 3: Configuration > Users

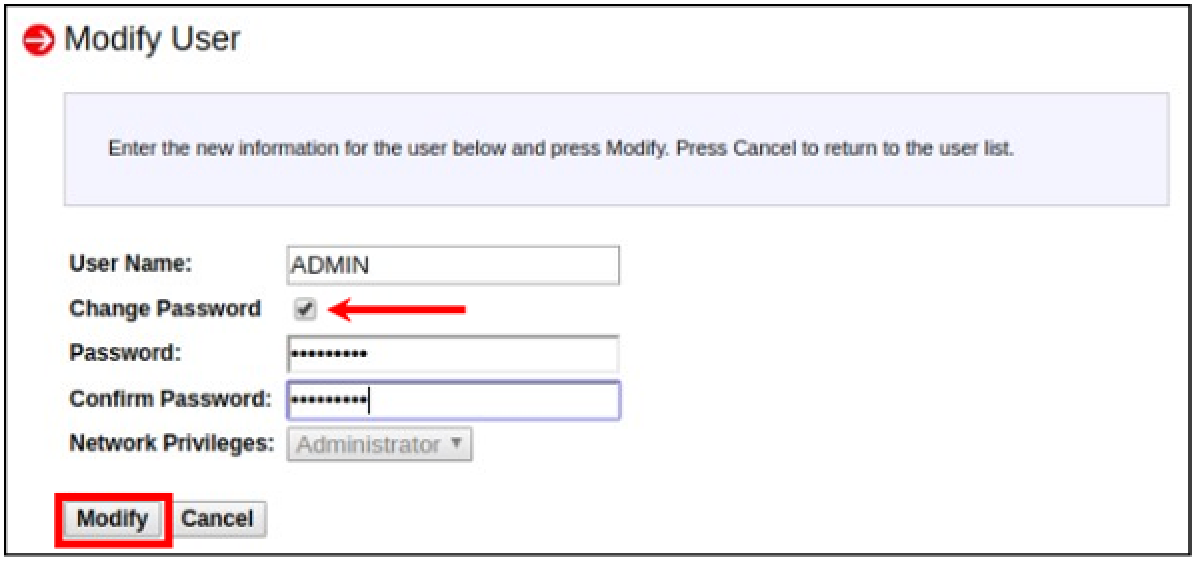

Users

The list below shows the current list of configured users. If you would like to delete or modify a user, select their name in the list and press Delete User or Modify User. To add a new user, select an unconfigured slot and press Add User.

Number of Configured Users: 2

User ID	User Name	Network Privilege
1	Anonymous	Reserved
2	ADMIN	Administrator
3	~	Reserved
4	~	Reserved
5	~	Reserved
6	~	Reserved
7	~	Reserved
8	~	Reserved
9	~	Reserved
10	~	Reserved

Fig. 4: Modify User



Modify User

Enter the new information for the user below and press Modify. Press Cancel to return to the user list.

User Name: ADMIN

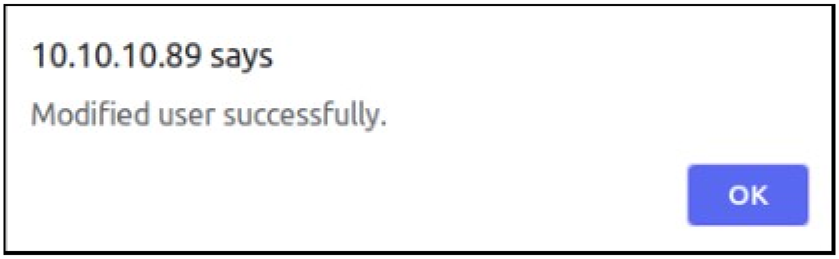
Change Password ☑

Password: ••••••••••

Confirm Password: ••••••••••

Network Privileges: Administrator

Fig. 5: Change Password and click Modify



10.10.10.89 says

Modified user successfully.

Fig. 6: Click OK

2.3.2 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
```

- List the current IPMI users

```
ipmitool user list
```

Note: Netgate appliances use the user name `ADMIN` 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      Unknown (0x00)
2   ADMIN            true    false      false      Unknown (0x00)
3                    true    false      false      Unknown (0x00)
4                    true    false      false      Unknown (0x00)
5                    true    false      false      Unknown (0x00)
6                    true    false      false      Unknown (0x00)
7                    true    false      false      Unknown (0x00)
8                    true    false      false      Unknown (0x00)
9                    true    false      false      Unknown (0x00)
10                   true    false      false      Unknown (0x00)
```

Warning: Usernames are case-sensitive.

- Reset the password for a user

  The default `ADMIN` 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
```

2.4 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.

- 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 1 ipaddr 172.31.123.5
  ipmitool lan set 1 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 1 defgw ipaddr 172.31.123.1
  ```

- Enable IPMI access on the interface

  ```
  ipmitool lan set 1 access on
  ```

- Unload the IPMI kernel module

  ```
  kldunload ipmi
  ```

2.5 Reinstalling pfSense Plus Software

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

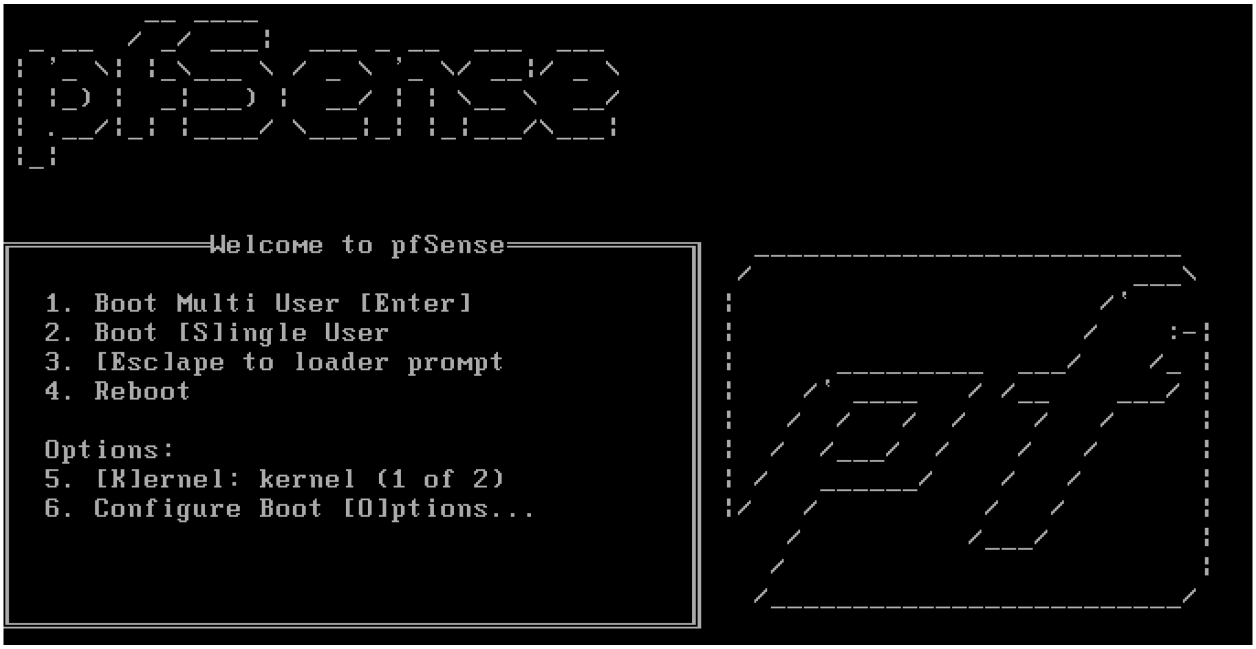
   Once the ticket is processed, the latest stable version of the firmware will be attached to the ticket, with a name such as:

   `pfSense-plus-memstick-23.09.1-RELEASE-amd64.img.gz`

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

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

3. *Connect to the console port* of the Netgate device.
4. Insert the memstick into an open USB port and boot the device.
5. After a minute the pfSense® Plus loader menu will be displayed with a 3 second timer. Either allow the menu to timeout or press `1` (the default) to continue.



```
Welcome to pfSense

 1. Boot Multi User [Enter]
 2. Boot [S]ingle User
 3. [Esc]ape to loader prompt
 4. Reboot

 Options:
 5. [K]ernel: kernel (1 of 2)
 6. Configure Boot [O]ptions...
```

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

```
Please choose the appropriate terminal type for your system.
Common console types are:
   ansi     Standard ANSI terminal
   vt100    VT100 or compatible terminal
   xterm    xterm terminal emulator (or compatible)
   cons25w  cons25w terminal
```

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

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

See also:

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

8. Once the installer is finished, choose `No` and press `Enter` to skip going to a shell.
9. The installer will then prompt to Reboot. Select **Reboot** and press `Enter`. The device will shutdown and reboot.

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

(continues on next page)

(continued from previous page)

```
Syncing disks, vnodes remaining... 0 0 done
All buffers synced.
Uptime: 5m43s
umass0: detached
umass1: detached
uhub1: detached
```

10. Remove the USB drive from the USB port.

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

See also:

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

2.6 Configuring an OPT interface as an additional WAN

Note: The default configuration has interfaces assigned as OPT ports, but the exact assignments vary based on the presence of expansion cards. See *Input and Output Ports* for specific default assignment layouts.

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

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 setup in some other way (e.g. VLANs).

- Click + **Add**

The firewall will assign the next available OPT interface number corresponding to the internal interface designation. For example, if there are no current OPT interfaces, the new interface will be **OPT1**. The next will be **OPT2**, and so on.

Note: As this guide does not know what that number will be on a given configuration, it will refer to the interface generically as **OPTx**.

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

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

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

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

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

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

- Click ⮅ Add to add a new rule at the top of the list.
- Configure the rule as follows:

  Interface Choose the new WAN interface (e.g. **WAN2**)

  Address Family *IPv4*

  Protocol *Any*

  Source *Network*, and fill in the LAN subnet, e.g. `192.168.1.0/24`.

    If there is more than one LAN subnet, create rules for each or use other methods such as aliases or CIDR summarization to cover them all.

Destination *Any*

Translation Address *Interface Address*

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

- Click **Save**
- Click **Apply Changes**

Repeat as needed for additional LANs.

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**, and WAN2 on **Tier 2**

  Description `Prefer WAN, fail to WAN2`

- Click **Save**
- Click ➕ **Add** to create another gateway group
- Configure the group as follows:

  Group Name `PreferWAN2`

  Gateway Priority Gateway for WAN on **Tier 2**, and WAN2 on **Tier 1**

  Description `Prefer WAN2, fail to WAN`

- Click **Save**
- Click ➕ **Add** to create another gateway group
- Configure the group as follows:

Group Name `LoadBalance`

Gateway Priority Gateways for WAN and WAN2 both on **Tier 1**

Description `Prefer WAN2, fail to WAN`

Note: This performs connection-based load balancing, not per-packet 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's important to ensure the firewall can always resolve hostnames using DNS even when running on a secondary WAN.

The needs here depend upon the configuration of the DNS Resolver or Forwarder.

If the DNS Resolver is in its default resolver mode, then default gateway switching will be sufficient to handle failover in most cases, though it may not be as reliable as using forwarding mode.

If the DNS Resolver is in forwarding mode or the firewall is using the DNS Forwarder instead, then maintaining functional DNS requires manually configuring gateways for forwarding DNS servers.

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

  These servers must be unique, the same server cannot be listed more than once.
- Select a gateway for each DNS server, corresponding to 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.
- 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 ↥ Add to add a new rule at the **top** of the list
- Configure the rule as follows:

  Action *Pass*

  Interface *LAN*

  Protocol *Any*

  Source *LAN net*

  Destination The other local subnet, VPN network, or an alias of such networks.

  Description `Pass to local and VPN networks`

  Do not set a gateway on this rule.
- Click **Save**
- Click **Apply Changes**

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's a good practice to have a separate DNS entry for each WAN and a shared entry for failover, or one per failover group. If that is not viable, at least have one for the most common needs.

The particulars of configuring Dynamic DNS entries vary by provider and are beyond the scope of this document.

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

2.7 Configuring an OPT interface as an additional LAN

Note: The default configuration has interfaces assigned as OPT ports, but the exact assignments vary based on the presence of expansion cards. See *Input and Output Ports* for specific default assignment layouts.

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

Configuring an additional LAN

2.7.1 Requirements

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

2.7.2 Assign the Interface

The first step is to assign an OPT interface.

- Navigate to **Interfaces > Assignments**

  Look at list of current assignments. If the interface in question is already assigned, there is nothing to do. Skip ahead to the interface configuration.

- Pick an available interface in **Available network ports**

  If there are no available interfaces, then one may need to be setup in some other way (e.g. VLANs).

- Click + **Add**

The firewall will assign the next available OPT interface number corresponding to the internal interface designation. For example, if there are no current OPT interfaces, the new interface will be **OPT1**. The next will be **OPT2**, and so on.

Note: As this guide does not know what that number will be on a given configuration, it will refer to the interface generically as **OPTx**.

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

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 IP address and CIDR mask for the new LAN

  For this example, `192.168.2.1/24`.

- **Do not** add or choose a gateway

- Uncheck **Block private networks**

  This interface is a private network, this option would prevent it from functioning.

- Uncheck **Block bogon networks**

  The rules on this interface should only allow traffic from the subnet on the interface, making this option unnecessary.

- Click **Save**
- Click **Apply Changes**

The lack of a selected gateway in the interface configuration causes the firewall to treat the interface as a LAN type interface.

The firewall uses LAN type interfaces as sources of outbound NAT traffic but does not apply outbound NAT on traffic exiting a LAN. The firewall does not add any extra properties on firewall rules to influence traffic behavior. The DNS Resolver will accept queries from clients on LAN type interfaces.

See also:

Interface Configuration

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.

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

  This sets the lower (**From**) and upper (**To**) bound of automatic addresses assigned to clients.

- The rest can be left at defaults
- Click **Save**

See also:

DHCPv4 Configuration

2.7.5 Outbound NAT

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

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

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

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

- Click ⤒ Add to add a new rule at the top of the list
- Configure the rule as follows:

Interface Choose the WAN interface. If there is more than one WAN interface, add separate rules for each WAN interface.

Address Family *IPv4*

Protocol *Any*

Source *Network*, and fill in the new LAN subnet, e.g. `192.168.2.0/24`.

Destination *Any*

Translation Address *Interface Address*

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

- Click **Save**
- Click **Apply Changes**

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

2.7.6 Firewall Rules

By default there are no rules on the new interface, so the firewall will block all traffic. This is not ideal for a LAN as generally speaking, the LAN clients will need to contact hosts through the firewall.

Rules for this interface can be found under **Firewall > Rules**, on the **OPTx** tab (or the custom name, e.g. **GUESTS**).

There are two common scenarios administrators typically choose for local interfaces: Open and Isolated

Open

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

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

- Navigate to **Firewall > Rules**, on the **OPTx** tab (or the custom name)
- Click Add to add a new rule at the top of the list
- Configure the rule as follows:

  Action *Pass*

  Interface *OPTx* (or the custom name) should already be set by default

  Protocol *Any*

  Source *OPTx Net* (or the custom name)

  Destination *Any*

  Description Text describing the rule, e.g. `Default allow all from OTPx`

- Click **Save**
- Click **Apply Changes**
- Add rule to pass any protocol from interface net to any destination

Isolated

In an isolated local network, hosts on the network cannot contact hosts on other networks unless explicitly allowed in the rules. Hosts can still contact the Internet as needed in this example, but that can also be restricted by more complicated rules.

This scenario is common for locked down networks such as for IOT devices, a DMZ with public services, untrusted Guest/BYOD networks, and other similar scenarios.

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

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

- Navigate to **Firewall > Aliases**
- Click + **Add**
- Configure it as follows:

  Name `PrivateNets`

  Description `Private Networks`

  Type *Network(s)*

- Add entries for:
  - `192.168.0.0/16`
  - `172.16.0.0/12`
  - `10.0.0.0/8`
- Click **Save**
- Navigate to **Firewall > Rules**, on the **OPTx** tab (or the custom name)

Add rule to pass DNS to firewall (or other DNS servers)

- Click ⤵ Add to add a new rule at the bottom of the list.
- Configure the rule as follows:

  Action *Pass*

  Interface *OPTx* (or the custom name)

  Protocol *TCP/UDP*

  Source *OPTx Net* (or the custom name)

  Destination *This Firewall (self)*

  If clients are to use DNS servers other than the firewall, use those as the destination instead.

  Destination Port Range *DNS*, or choose *Other* and enter `53`

  To allow DNS over TLS as well, add another rule for DNS over TLS or port `853`.

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

- Click **Save**

Add rule to pass ICMP to firewall

- Click Add to add a new rule at the bottom of the list.
- Configure the rule as follows:

Action *Pass*

Interface *OPTx* (or the custom name)

Protocol *ICMP*

ICMP Subtype *Any* is OK in this case, ICMP is useful but some people prefer to limit to *Echo Request* only to allow ping and nothing else.

Source *OPTx Net* (or the custom name)

Destination *This Firewall (self)*

Description `Allow client ICMP to the firewall`

- Click **Save**

Add rule to reject any other traffic to firewall

- Click Add to add a new rule at the bottom of the list.
- Configure the rule as follows:

Action *Reject*

Interface *OPTx* (or the custom name)

Protocol *Any*

Source *Any*

Destination *This Firewall (self)*

Description `Reject all other traffic to the firewall`

- Click **Save**

Add rule to reject traffic from this network to private networks

- Click Add to add a new rule at the bottom of the list.
- Configure the rule as follows:

Action *Reject*

Interface *OPTx* (or the custom name)

Protocol *Any*

Source *Any*

Destination *Single Host or Alias*, `PrivateNets` (the alias created earlier)

Description `Reject all other traffic to private networks`

- Click **Save**

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

- Click ⤵ Add to add a new rule at the bottom of the list.
- Configure the rule as follows:

  Action *Pass*

  Interface *OPTx* (or the custom name)

  Protocol *Any*

  Source *OPTx Net* (or the custom name)

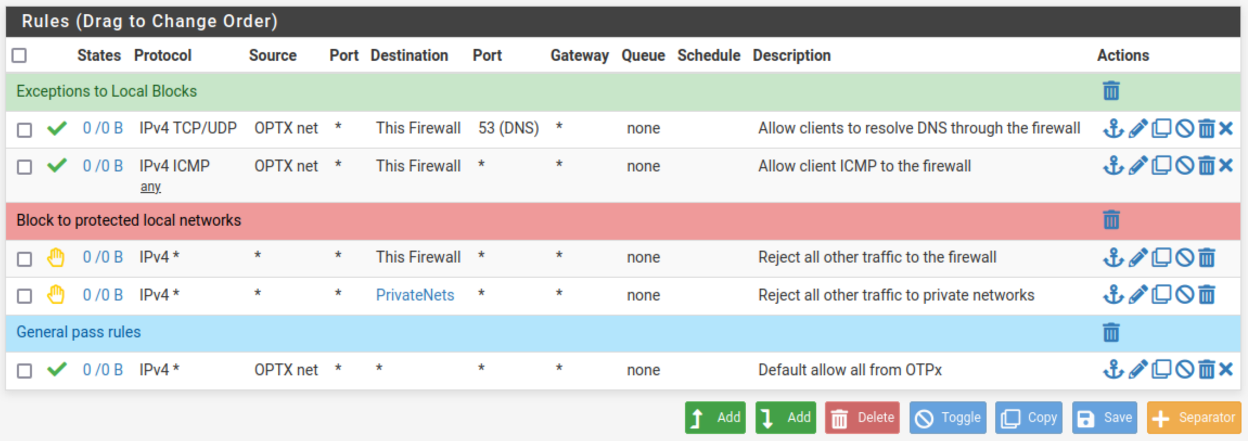
  Destination *Any*

  Description `Default allow all from OTPx`

- Click **Save**

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

After the configuration, the rules should look like the following figure:



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Exceptions to Local Blocks												🗑
□	✓	0 /0 B	IPv4 TCP/UDP	OPTX net	*	This Firewall	53 (DNS)	*	none		Allow clients to resolve DNS through the firewall	⚓✎❐⊘🗑✕
□	✓	0 /0 B	IPv4 ICMP any	OPTX net	*	This Firewall	*	*	none		Allow client ICMP to the firewall	⚓✎❐⊘🗑✕
Block to protected local networks												🗑
□	✋	0 /0 B	IPv4 *	*	*	This Firewall	*	*	none		Reject all other traffic to the firewall	⚓✎❐⊘🗑
□	✋	0 /0 B	IPv4 *	*	*	PrivateNets	*	*	none		Reject all other traffic to private networks	⚓✎❐⊘🗑
General pass rules												🗑
□	✓	0 /0 B	IPv4 *	OPTX net	*	*	*	*	none		Default allow all from OTPx	⚓✎❐⊘🗑✕

Fig. 7: Example firewall rules for isolated LAN type segment

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

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

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 get out to the Internet. However, there may be other custom settings which need accounted for when adding a new local interface:

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

2.8 Factory Reset Procedure

The Netgate 1537 firewall appliance does not have a hardware button to reset the configuration to factory defaults. On this device it is still possible to perform a Factory Reset from GUI or Console.

See also:

- Factory Reset from GUI or Console

The linked document has complete details but the procedure can be summarized as follows:

Reset from the console:

- *Connecting to the Console Port* or SSH
- Choose menu option `4` to reset to factory defaults
- Confirm the action and allow the appliance to reboot

Reset from the GUI:

- Navigate to **Diagnostics > Factory Defaults** to perform the reset.

CHAPTER

THREE

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.