## OUT OF THE BOX

1. Getting Started ........................................... 2
2. Input and Output Ports ................................. 13
3. Safety and Legal ........................................... 17
4. Configuring the Switch Ports ......................... 26
5. Connecting to the Console Port ...................... 41
6. Reinstalling pfSense Software ....................... 48
7. M.2 SATA Installation ..................................... 50
8. Expansion Card Installation .......................... 60
9. BIOS Flash Procedure ..................................... 72
10. Switch Ports Overview ................................ 73
11. Additional Resources ................................... 78
12. Warranty and Support .................................. 79
This Quick Start Guide covers the first time connection procedures for the Netgate® XG-7100 1U Firewall Appliance and will provide the information needed to keep the appliance up and running.
The basic firewall configuration begins with connecting the pfSense® appliance to the Internet. Neither the modem nor the pfSense 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 pfSense 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 pfSense 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 pfSense appliance. Connect the other end to the network connection on the computer. In order to access the web configurator, 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 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 pfSense appliance are powered up, the next step is to power up the computer.

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

### 1.2 Logging Into the Web Interface

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

Username admin
Password pfsense

Click Login to continue

1.3 Wizard

Upon successful login, the following is displayed.
1.4 Configuring Hostname, Domain Name and DNS Servers

1.5 Hostname

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

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

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

1.6 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.

1.7 DNS Servers

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

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

1.8 Time Server Configuration

![Time Server Information](image)

1.9 Time Server Synchronization

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

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.

1.11 Configuring Wide Area Network (WAN) Type

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

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

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

### 1.12 MAC Address

![MAC Address](image)

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

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

### 1.13 Configuring MTU and MSS

![MTU and MSS](image)

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.
1.14 Configuring DHCP Hostname

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

1.15 Configuring PPPoE and PPTP Interfaces

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

When enabled, all private network traffic originating on the internet is blocked.

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

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

- 10.0.0.1 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.
1.17 Configuring LAN IP Address & Subnet Mask

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

Click Next to continue.

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

1.18 Change Administrator Password

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

Click **Reload** to save configuration.

1.20 Basic Firewall Configured

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

1.21 Backing Up and Restoring

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

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

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

See also:

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

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

INPUT AND OUTPUT PORTS

2.1 Ethernet Ports

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Port Name</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN</td>
<td>ETH1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>LAN</td>
<td>ETH2-ETH8</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>OPT1</td>
<td>IX0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>OPT2</td>
<td>IX1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

2.1.1 Switched Ethernet Ports (ETH1-ETH8)

ETH1-8 are switched ports sharing 5 Gbps (2x 2.5 Gbps) to the Intel SoC. These ports can be isolated as an independent interface with the configuration of VLAN tagging as shown in Switch Ports Overview.

Tip: Best Practice: Use the ports on the 4-port Network Interface Card for the High Availability (HA) connections (WAN, LAN, and Sync) on this product for complete failover and redundancy. For more information, review the High Availability section of the XG-7100 Switch Overview page.

Warning: LAGG has limited support currently on the ethernet switchports (Load Balance mode only). For more information, review the Switch LAGG section of the XG-7100 Switch Overview page.
2.1.2 SFP+ Ethernet Ports (IX0-IX1)

IX0-IX1 are discrete ports, each with dedicated 10 Gbps back to the Intel SoC.

Below are some general guidelines for compatible SFP/SFP+ modules:

- Intel-branded SFP+ SR/LR Dual Speed (1G/10G) optical modules.  
  
- Intel-branded SFP+ DA twin-ax cables that comply with SFF-8431 v4.1 and SFF-8472 v10.4 specifications. **Note:** Limited to 10G link speed (no 1G support).

- Third party SFP+ DA twin-ax cables that comply with SFF-8431 v4.1 and SFF-8472 v10.4 specifications. **Note:** Limited to 10G link speed (no 1G support).

- SFP+ AoCs (Active optical Cables). **Note:** Limited to 10G link speed (no 1G support).

- Third party SFP+ SR/LR dual speed 1G/10G) optical modules

- SFP+ active copper cables

- 1000BASE-SX / 1000BASE-LX optical modules

Specific known-working modules include:

<table>
<thead>
<tr>
<th>Model / Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finisar FTLF1318P3BTL</td>
<td>1000BASE-LX and 1G Fibre Channel (1GFC) 10km Industrial Temperature Gen 3 SFP Optical Transceiver</td>
</tr>
<tr>
<td>Finisar FTLX1471D3BCL</td>
<td>10Gb/s 10km Single Mode Datacom SFP+ Transceiver</td>
</tr>
<tr>
<td>Intel FTLX8571D3BCV-IT</td>
<td>1G/10G Dual Rate SFP Fiber Optical Transceiver Module</td>
</tr>
<tr>
<td>Finisar FTLX8574D3BCL</td>
<td>10GBASE-SR/SW 400m Multimode Datacom SFP+ Optical Transceiver</td>
</tr>
<tr>
<td>Finisar FTLF8519P3BNL</td>
<td>1000BASE-SX and 2G Fibre Channel (2GFC) 500m Extended Temperature SFP Optical Transceiver <strong>Note:</strong> Links at 1G, 2G is not supported</td>
</tr>
</tbody>
</table>

**Warning:** The ix(4) driver used for ports IX0-IX1 does not support ALTQ traffic shaping directly. Limiters or tagged VLAN interfaces may be used for ALTQ traffic shaping.
Warning: There is an Intel-supplied driver issue for the C3000, preventing 1Gbps and 10Gbps copper modules from being recognized on the SFP+ ports. Copper modules are not supported.

2.2 Optional 4-Port Intel 1 Gbps Ethernet Expansion Card

<table>
<thead>
<tr>
<th>Num</th>
<th>Interface Name</th>
<th>Port Name</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OPT3</td>
<td>igb0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>1</td>
<td>OPT4</td>
<td>igb1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>OPT5</td>
<td>igb2</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>OPT6</td>
<td>igb3</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

2.3 Optional 2-Port Intel 1 Gbps Ethernet Expansion Card

<table>
<thead>
<tr>
<th>Num</th>
<th>Interface Name</th>
<th>Port Name</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OPT3</td>
<td>igb0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>1</td>
<td>OPT4</td>
<td>igb1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

2.4 Other Ports, Buttons, and Indicators

- Semi-recessed Power (PWR) (performs a graceful shutdown of pfSense® software)
- Recessed Reset Button (performs a hard reset, immediately turning the system off)
- 1x USB 3.0
- Status LED
- Power (PWR) LED (green when powered on, red after a graceful shutdown)
- Console (Mini-USB)
- 2x USB 2.0
Note: When a graceful shutdown is performed, the XG-7100 Power (PWR) LED will turn red but will stay lit. The Ethernet activity LEDs will turn off. The power supply fan will continue to run. Turning off the rocker switch on the back of the power supply will eliminate all power to the system.

The power button should be depressed 3-5 seconds to initiate a graceful shutdown or to power on the device when the PWR LED is red.

Warning: A hard reset of the system could cause data corruption and should be avoided. Halt or reboot the system through the console menu or the web configurator to avoid data corruption.
CHAPTER THREE

SAFETY AND LEGAL

• Safety Notices
• Electrical Safety Information
• FCC Compliance
• Industry Canada
• Australia and New Zealand
• CE Marking
• RoHS/WEEE Compliance Statement
  – English
  – Deutsch
  – Español
  – Français
  – Italiano
• Declaration of Conformity
  – Česky [Czech]
  – Dansk [Danish]
  – Nederlands [Dutch]
  – English
  – Eesti [Estonian]
  – Suomi [Finnish]
  – Deutsch [German]
  – Ελληνικά [Greek]
  – Magyar [Hungarian]
  – Íslenska [Icelandic]
  – Italiano [Italian]
  – Latviski [Latvian]
  – Lietuviškai [Lithuanian]
3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 Australia and New Zealand

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

3.6 CE Marking

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

3.7 RoHS/WEEE Compliance Statement

3.7.1 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.

3.7.2 Deutsch


3.7.3 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.

3.7.4 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.

3.7.5 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.
3.8 Declaration of Conformity

3.8.1 Česky [Czech]

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

3.8.2 Dansk [Danish]

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

3.8.3 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.

3.8.4 English

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

3.8.5 Eesti [Estonian]

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

3.8.6 Suomi [Finnish]

NETGATE vakuuttaa täten että NETGATE device, tyyppinen laite on direktiivin 1999/5/EY pohjusmukainen 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.

3.8.7 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)

3.8.8 Ελληνικά [Greek]

ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΝΕΤΓΑΤΕ ΔΗΛΩΝΕΙ ΌΤΙ ΝΕΤΓΑΤΕ device, ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1995/5/ΕΚ.
3.8.9 Magyar [Hungarian]

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

3.8.10 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.

3.8.11 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.

3.8.12 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.

3.8.13 Lietuviškai [Lithuanian]

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

3.8.14 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.

3.8.15 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.

3.8.16 Slovensky [Slovak]

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

3.8.17 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.
3.8.18 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.

3.8.19 Polski [Polish]

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

3.8.20 Português [Portuguese]

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

3.8.21 Română [Romanian]

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

3.9 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.
3.10 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.

3.11 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.

3.12 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.

3.13 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 FOUR

CONFIGURING THE SWITCH PORTS

See also:
For an overview of how the switch ports are set up, see Switch Ports Overview.

4.1 Switch Section

From the pfSense webGUI, there is a menu option called Switches under the Interfaces drop-down. This section contains switch specific configuration options.

Selecting Switches from the drop-down will bring up the Switch page with four sections:
4.1 System

4.1.1 System

4.1.2 LAGGs

4.1.3 Ports

Information on switchport status and port names. If 802.1q is enabled, this section can also be used to specify the native VLAN ID for each port. The Port VID defined will be used to tag inbound untagged traffic.

4.1.4 VLANs

Enable/Disable 802.1q VLAN mode. Configure VLAN access/trunk interfaces with 802.1q or configure port groups with Port VLAN Mode.

4.2 Interfaces Section

There is also relevant configurations under Interfaces -> Assignments.

4.2.1 Interface Assignments

Under Interface Assignments, notice LAGG0 (UPLINK) is displayed as an available port but is not enabled in the list of interfaces. This is because the default configuration is only expecting VLAN tagged traffic so the VLAN child interface 4090 and 4091 are enabled instead.
Fig. 3: 802.1q enabled (default)

Fig. 4: Port VLAN Mode
Fig. 5: 802.1q enabled (default)

Fig. 6: Port VLAN Mode
4.2.2 VLANs

Under VLANs, the default WAN and LAN VLAN can be seen. Additional VLAN networks that will be used by the switch should be defined here with lagg0 as the parent interface.

Any additional VLAN interface added to the switch should also be added, enabled, and configured under Interface Assignments. Firewall rules will also be needed for new interfaces added.

4.2.3 LAGGs

Under LAGGs, the default lagg0 containing ix2 and ix3 can be seen. The lagg0 interface should not be modified.
4.3 Switch Configuration Examples

4.3.1 Dedicated LAN switch

In this scenario, SFP+ port ix0 will be configured as the WAN interface. ETH1-8 will be configured as a LAN switch.

For this specific example, I’ll perform the WAN interface reassignment over console. Re-assigning the WAN can be done from the webGUI as well.

This is what the default interface assignments look like on a XG-7100 without an addon NIC:

```
*** Welcome to pfSense 2.4.3-RELEASE (amd64) on pfSense ***

WAN (wan)  -> lagg0.4090  -> v4/DHCP4: 10.10.30.18/24
LAN (lan)  -> lagg0.4091  -> v4: 192.168.1.1/24
OPT1 (opt1)  -> ix0  ->
OPT2 (opt2)  -> ix1  ->

0) Logout (SSH only)  9) pfTop
1) Assign Interfaces  10) Filter Logs
2) Set interface(s) IP address  11) Restart webConfigurator
3) Reset webConfigurator password  12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system  14) Enable Secure Shell (sshd)
6) Halt system  15) Restore recent configuration
7) Ping host  16) Restart PHP-FPM
8) Shell

Enter an option:  
```

In this example, ix0 will be WAN, so select option 1 to re-assign WAN from lagg0.4090 to ix0:

```
Enter an option: 1

Valid interfaces are:

ix0  00:a0:c9:60:00:00:00 (down) Intel(R) PRO/10GbE PCI-Express Network Driver,
ix1  34:12:78:56:01:01 (down) Intel(R) PRO/10GbE PCI-Express Network Driver,
ix2  00:a0:c9:60:00:02 (down) Intel(R) PRO/10GbE PCI-Express Network Driver,
ix3  00:a0:c9:60:00:00:02 (down) Intel(R) PRO/10GbE PCI-Express Network Driver,

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]? 
```

No additional VLANs are needed for this, so enter n to continue.

Input ix0 as the new WAN interface name:
Should VLANs be set up now [y|n]? n

VLAN interfaces:

lagg0.4090  VLAN tag 4090, parent interface lagg0
lagg0.4091  VLAN tag 4091, parent interface lagg0

If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection (ix0 ix1 ix2 ix3 lagg0.4090 lagg0.4091 or a): 

Enter the LAN interface name or 'a' for auto-detection (ix0 ix1 ix2 ix3 lagg0.4090 lagg0.4091 or a): ix0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(ix1 ix2 ix3 lagg0.4090 lagg0.4091 a or nothing if finished): lagg0.4091

Optional interface 1 description found: OPT1
Enter the Optional 1 interface name or 'a' for auto-detection (ix1 ix2 ix3 lagg0.4090 a or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> ix0
LAN  -> lagg0.4091

Do you want to proceed [y|n]? 

The interface assignments should show like this now:
At this point SFP+ port **ix0** is now configured as the WAN interface. The LAN interface is still configured the same as the default. Next, the switch will need to be updated so that ETH1 (previously WAN) acts the same as ETH2-8. This will be done from the webGUI.

From the webGUI, pull up the Switch VLAN configuration under **Interfaces -> Switches -> VLANs**:

VLAN 4090 is no longer needed since **WAN** is dedicated to **ix0** now. You can either select **4090** on the row containing VLAN 4090 to delete this entry, or click **to remove port 1 as a member:**
For this example, I simply removed VLAN 4090 from the switch with ![Image]. Now edit the VLAN 4091 entry to include Member 1 as shown below:

![Image]

Next, update the PVID for ETH1 so that it uses VLAN 4091 rather than the old VLAN 4090. To do this, click on the **Ports** tab and click on the 4090 Port VID to modify it:
Then click on Save:

At this point, everything should be configured properly. ETH1-8 will act as a single LAN switch. One final step that should be performed is to remove the old VLAN 4090 from pfSense. So far VLAN 4090 was only removed from the switch. To remove the old VLAN, go to Interfaces -> Assignments -> VLANs and use \(\text{Remove} \) on the 4090 row to remove this VLAN interface:

4.3.2 Two LAN switches

In this scenario, the LAN switch from the previous example will be split into two LAN switches.

A new LAN network should be created in pfSense first. Similar to the existing LAN interface, another VLAN interface should be used so the switch can segment traffic appropriately.

Create a new VLAN with lagg0 as the parent under Interfaces -> Assignments -> VLANs:
Once the VLAN has been created, it should look something like this:

Add, enable, and configure the VLAN interface under Interfaces Assignments:
Also create any necessary firewall rules under **Firewall -> Rules**.

Now that pfSense knows of this new VLAN network, configure the switch so that ETH1-4 use the new network. To do this, go to **Interfaces -> Switches -> VLANs** and click the **Add Tag** button. Input the VLAN tag for the new network (same as the VLAN ID configured in the previous steps) and add ETH1-4 and PORT9-10 (uplinks) as members. Be sure **9** and **10** are marked as **tagged**.
Once this is done, delete the untagged members 1, 2, 3, 4 from VLAN group 2 and click the **Save** button. The final result should look like this:

Lastly, update the Port VIDs to use the new 4081 VLAN rather than 4091 on ETH1-4 and click **Save**:
Now ETH1-4 act as a switch for the VLAN 4081 LAN and ETH5-8 act as a switch for the VLAN 4091 LAN.

### 4.3.3 Trunking VLAN tagged traffic

For expanding on the previous example, let’s assume there is a management VLAN of 4000 where devices are already tagged on this VLAN prior to hitting pfSense. Devices on this VLAN may come through on ETH8 but there may also be untagged client traffic.

First, create the management VLAN of 4000 in pfSense using the same steps in the previous example (up to the switch configuration part). Next, add the VLAN to the switch under Interfaces -> Switches -> VLANs. ETH8 and PORT9-10 should be added as members and all three will be marked as tagged:

Once it’s added, the final result should look like this:
Untagged traffic on ETH8 will be assigned a VLAN ID of 4091. ETH8 and the uplinks will also accept traffic that has already been tagged with a VLAN ID of 4000 as well.
There are times when directly accessing the console is required. Perhaps webGUI or SSH access has been locked out, or the password has been lost or forgotten. This guide shows how to regain access directly through the console.

5.1 Simple Configuration

Below are the simple instructions for connecting to the console port with Microsoft Windows. If these steps do not work for you or if you’re an operating system other than Windows, then please skip forward to Advanced Configuration.

5.1.1 Serial Terminal Emulation Client

A serial terminal emulation program is required to access the pfSense® appliance console through the serial interface. PuTTY is free and recommended.

5.1.2 Configuring Serial Terminal Emulator

PuTTY must be configured to communicate with the pfSense appliance. In order to do so, you must first know what COM Port your computer has assigned to your serial port. Even if you assigned your serial port to COM1 in the BIOS, Windows may remap it to a different COM Port.

To determine this, you must open Windows Device Manager and view the COM port assignment:
Note: The first time you connect your computer to the pfSense appliance, it may take up to 3 minutes for the driver to install. It should install automatically for Windows 7 and above.

Open PuTTY and locate the Session display as shown below. Set Serial line to the COM Port that is displayed in Windows Device Manager, COM3 for this example, and the Speed to 115200 bits per second, the speed of the BIOS in this case. For the Connection type, select Serial.
Click the Open button and the console screen will be displayed.

5.2 Advanced Configuration

A Silicon Labs CP210x USB-to-UART bridge driver is used to provide access to the console, which is exposed via the USB Mini-b (5-pin) port on the appliance.

5.2.1 Install the Driver

Install an appropriate Silicon Labs CP210x USB to UART Bridge driver on the workstation used to connect with the system if needed. There are drivers available for Windows, Mac OS X, and Linux available for download.
5.2.2 Connect a USB Cable

Next, locate an appropriate USB cable that has a USB Mini-b (5-pin) connector on one end and a regular USB (Type A) plug on the other end. These cables are commonly used with smaller USB peripherals such as GPS units, cameras, and so on.

Gently push the USB Mini-b (5-pin) plug end into the console port on the appliance and connect the USB type A plug into an available USB port on the workstation.

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

5.2.3 Locate the Console Port Device

The appropriate device to attach the terminal program to each platform varies by platform and must be located before attempting to connect to the console.

**Windows**

To locate the device name on Windows, open Device Manager and expand the section for Ports (COM & LPT). Look for an entry with a title such as Silicon Labs CP210x USB to UART Bridge. If there is a label in the name that contains “COMX” where X is a decimal digit (e.g. COM1), that value is what would be used as the port in the terminal program.

![Device Manager screenshot]

**Mac OS X**

The device associated with the system console is likely to show up as /dev/cu.SLAB_USBtoUART.

**Linux**

The device associated with the system console is likely to show up as /dev/ttyUSB0. Look for messages about the device attaching in the system log files or by running dmesg.

**Note:** If the device does not appear in /dev/, see the note above in the driver section about manually loading the Linux driver and then try again.

**FreeBSD**

The device associated with the system console is likely to show up as /dev/cuaU0. Look for messages about the device attaching in the system log files or by running dmesg.
5.2.4 Launch a Terminal Program

Use a terminal program to connect to the system console port. PuTTY is a popular terminal program that is available on various operating systems. Some other choices of terminal programs:

- Linux: screen, PuTTY, minicom, dterm
- Mac OS X: screen, ZTerm, cu
- Windows: PuTTY, SecureCRT, Do not use Hyperterminal
- FreeBSD: screen, cu

The settings to use within the terminal program are:

**Speed** 115200 baud

**Data bits** 8

**Parity** none

**Stop bits** 1

**Flow Control** Off or XON/OFF. Hardware flow control (RTS/CTS) must be disabled.

Client-Specific Examples

**PuTTY**

Launch PuTTY and configure it for a **Serial** type connection with a speed of **115200** using the port name located previously.

- **Windows Example:**

- **Linux Example:**

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

**Window**  Columns x Rows = 80x24

**Window > Appearance**  Font = *Courier New 10pt or Consolas 10pt*
**Window > Translation**  Remote Character Set = *Use font encoding* or *UTF-8*

**Window > Translation**  Handling of line drawing characters = *Use font in both ANSI and OEM modes*  
*or Use Unicode line drawing code points*

**Window > Colours**  Indicate bolded text by changing = The colour

**GNU screen**

In many cases *screen* may be invoked simply by using the proper command line:

- Mac OS X
  
  `sudo screen /dev/cu.SLAB_USBtoUART 115200`

- Linux
  
  `sudo screen /dev/ttyUSB0 115200`

- FreeBSD
  
  `sudo screen /dev/cuaU0 115200`

If portions of the text are unreadable but appear to be properly formatted, the most likely culprit is a character encoding mismatch in the terminal. For example, on OS X this is commonly required

`sudo screen -U /dev/cu.SLAB_USBtoUART 115200`

Adding the `-U` parameter to the *screen* command line arguments forces it to use UTF-8 for character encoding.

### 5.3 Troubleshooting

#### 5.3.1 No Serial Output

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

- Ensure the cable is correctly attached and fully inserted
- Ensure the terminal program is using the correct port
- Ensure the terminal program is configured for the correct speed. The default BIOS speed is 115200, and many other modern operating systems use that speed as well. Some older operating systems or custom configurations may use slower speeds such as 9600 or 38400.
- Ensure the operating system is configured for the proper console (e.g. *ttyS1* in Linux). Consult the various operating install guides on this site for further information.

#### 5.3.2 Garbled Serial Output

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

- Ensure the terminal program is configured for the correct speed. (See “No Serial Output” above)
- Ensure the terminal program is configured for the proper character encoding, such as UTF-8 or Latin-1, depending on the operating system. (See the previous entry under “GNU screen”)

© Copyright 2020 Rubicon Communications LLC 46
5.3.3 Serial Output Stops After the BIOS

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

- Ensure the terminal program is configured for the correct speed for the installed operating system. (See “No Serial Output” above)
- Ensure the installed operating system is configured to activate the serial console.
- Ensure the installed operating system is configured for the proper console (e.g. `ttyS1` in Linux). Consult the various operating install guides on this site for further information.
- If booting from a USB flash drive, ensure that the drive was written correctly and contains a bootable operating system image.
1. Please open a support ticket to request access to the factory firmware by selecting **Firmware Access** as the **General Problem** and then select **Netgate XG-7100 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-netgate-memstick-XG-7100-2.4.4-RELEASE-p3-amd64.img.gz`

**Note:** The pfSense® factory version is the version that is preinstalled on units purchased from Netgate. The factory image is optimally tuned for our hardware and contains some features that cannot be found elsewhere, such as the AWS VPN 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 pfSense device.

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

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

6. Console options are presented for serial console installation. The default option is **vt100**.

   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

   **Note:** Choosing the default **vt100** will work, but using **cons25w** on the XG-7100 will be easier to read.

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

   **Note:** Options such as the type of disk partition can be modified through this installation if required.
8. The installer will then prompt to choose the type of system being installed, which pre-configures device-specific defaults. Choose the option that exactly matches the unit being reinstalled. If the model is unknown, check the sticker on the bottom of the unit.

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

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

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

11. Remove the USB drive from the USB port. pfSense will restart automatically. 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.

**Note:** For information on restoring from a previously saved configuration, go to Backup and Restore.
The XG-7100 1U has 32 GB of onboard eMMC storage. Optionally, a M.2 SATA drive can be installed as an upgrade or to bypass the onboard eMMC flash memory.

**Warning:** Before proceeding:

1. Backup your configuration file, if possible.
2. Unplug the system for at least 60 seconds to ensure all phantom power has dissipated.
3. Anti-static protection must be used throughout this procedure.
4. Any hardware damage incurred during this procedure is not covered by the hardware warranty.

**Note:** By default, the M.2 SATA drive will be the first drive recognized by pfSense® software. pfSense must be reinstalled on the M.2 SATA drive.

**Note:** The XG-7100 1U does not support NVMe drives.

The M.2 SATA slot is located underneath the XG-7100 system board, so the entire board must be removed. The standoff is for the 80mm M.2 SATA drive.

1. Remove the seven (7) lid screws and remove the lid.

   **Note:** Some systems may only have six (6) lid screws.

2. Unplug the Power Supply Connector from the system board, being careful not to flex the board.

   **Warning:** Be sure to pull from the connector, not the wires.

3. Unplug the fans from the system board, being careful not to flex the board.

   **Warning:** Be sure to pull from the connectors, not the wires.

4. Remove the four (4) system board screws and gently slide system board away from the front faceplate until the board is free.
5. Turn the board over and locate the M.2 SATA slot.
6. Insert the gold leads of the M.2 SATA drive into the slot at the angle shown.

**Note:** Be sure the drive label is facing up and can be seen. The drive slot is keyed and the drive can only go in one way. Do not force the drive into the slot.

7. Push the M.2 SATA drive down until it is parallel with the system board and use the screw to secure the M.2 SATA drive in place.
8. Turn the board over and place it into the chassis. Secure the system board with four (4) board screws.
9. Replace the power supply connector and fan connectors.
10. Replace the lid and lid screws. Be sure the L-Bracket is not pinched by the lid.
11. Reinstall the pfSense software on the new M.2 SATA drive.
12. Restore your configuration backup if you have one.
Fig. 2: Power Supply Connector Location
Fig. 3: Fan Connector Locations
Fig. 4: Board Screw Locations
Fig. 5: M.2 SATA Slot Location
Fig. 6: M.2 SATA Drive Properly Inserted into the Slot
Fig. 7: Secure the M.2 SATA Drive
Fig. 8: M.2 SATA Drive Installed
Fig. 9: Proper Placement of the Lid and L-Bracket
EXPANSION CARD INSTALLATION

The XG-7100 1U has a x4 PCIe expansion bus. By default, the expansion card riser and extender are not installed unless purchased separately with an expansion card.

**Warning:** Before proceeding:

1. Backup your configuration file.
2. Unplug the system for at least 60 seconds to ensure all phantom power has dissipated.
3. Anti-static protection must be used throughout this procedure.
4. Any hardware damage incurred during this procedure is **not covered** by the hardware warranty.

The XG-7100 PCIe Installation Kit from Netgate includes the components pictured below. This kit does not include the actual expansion card to be installed.

![Bracket, Screws, Riser, and Extender](image)

*Fig. 1: Bracket, Screws, Riser, and Extender*

When installing an optional expansion card, first install the riser and extender using the riser mounting bracket.

1. Remove the seven (7) lid screws and remove the lid.
2. Remove the faceplate by unscrewing the 4 black faceplate screws.

3. Remove the L-Bracket behind the faceplate blank by unscrewing 1U Lid screw (M3x0.5 6MM Long Flat Head).

   **Note:** Notice that the L-Bracket is behind the Faceplate Blank, locking it into place.

4. Remove the faceplate blank.
5. Using Long Board Mount Screws, attach the riser card to the mounting bracket.
6. Line up the riser with the connector and insert the riser into the slot.
7. Attach the bracket to the chassis using Short Board Mount Screws.
8. Line up the extender and insert it into the riser.

   **Warning:** The connection is keyed and the riser will only go in one way. Do not force it.
Fig. 4: The L-Bracket and Screw
Fig. 5: Remove the L-Bracket and Screw
9. Carefully align the expansion card with the extender.
10. Insert the Expansion Card fully into the extender.
11. Place the L-Bracket behind the expansion card and screw into place using a Lid Screw.
12. Reattach the faceplate with 4 black faceplate screws.
13. Replace the lid.
Fig. 7: Attach Riser to Bracket
Fig. 8: Align the Riser to the Connector and Insert
Fig. 9: Attach the Bracket to the Chassis
Fig. 10: Line up the Extender with the Riser as shown

Fig. 11: Extender seated into the Riser
Fig. 12: Align Expansion Card with Extender
Fig. 13: Insert Expansion Card
Fig. 14: Secure the Expansion Card with the L-Bracket
9.1 Update via the GUI

**Warning:** This only works with Netgate systems running pfSense® version 2.3 or greater.

1. To install the package, navigate to **System > Package Manager > Available Packages**.
2. Click the **Install** button for the package named **Netgate_Coreboot_Upgrade**.
3. On the next page, click the **Confirm** button.
4. When the installation is complete a message will appear saying:

```
pfSense-pkg-Netgate_Coreboot_Upgrade installation successfully completed
```

5. Now that the package is installed, navigate to **System > Netgate Coreboot Upgrade**.
6. This page will show you the latest version of Coreboot available and the current version that is running on the system. If you happen to be on an older version of Coreboot then an **Update** button will be available to click.

**Important:** Pay close attention to any disclaimers presented. Some devices require a physical reboot or some step unique to that device.
SWITCH PORTS OVERVIEW

10.1 Interface Links

In addition to two SFP+ interfaces, there is also an ethernet switch on the XG-7100. There are eight ethernet ports on this switch that are physically accessible - these interfaces are referred to as ETH1-ETH8. In addition to those 8 ports, there are also three additional ports that operate behind the scenes - PORT 0, PORT 9 (ix2), and PORT 10 (ix3).

ETH1-ETH8 are gigabit switchports.

PORT 9-10 are 2.5 Gbps uplink switchports. These two ports connect the ethernet switch to a Denverton SoC. The SFP+ interfaces (ix0 and ix1) also connect to this SoC.

The diagram below demonstrates how these interfaces are connected:
From the operating systems perspective, there are four physical interfaces present:

<table>
<thead>
<tr>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ix0</td>
</tr>
<tr>
<td>ix1</td>
</tr>
<tr>
<td>ix2</td>
</tr>
<tr>
<td>ix3</td>
</tr>
</tbody>
</table>

**ix0** - 10Gbps SFP+

**ix1** - 10Gbps SFP+

**ix2** - 2.5 Gbps (2500-Base-KX, switch link to SoC/CPU)

**ix3** - 2.5 Gbps (2500-Base-KX, switch link to SoC/CPU)

### 10.2 High Availability

Switched Ethernet ports can be used for High Availability (HA), but there is one limitation when configuring switchports for HA. Because the uplinks from the switch to the SoC are always up, failover is only effective in scenarios where a system completely dies. If a single switch interface goes down, CARP will not be able to detect this properly so the PRIMARY will remain PRIMARY on any switch interfaces that drop link.

The SECONDARY will also consider itself PRIMARY of the network associated to the switch link that dropped. In this situation, LAN clients will likely go through the SECONDARY but will not be able to get online if NAT is utilized with a WAN CARP IP. It’s possible to NAT to the WAN interface IP to get around this but it can cause state issues during failover.

**For best results**, use the ports on a Network Interface expansion card. When configured correctly, the discrete ports of the add-in NIC will provide full redundancy and failover in the event of a network outage or scheduled maintenance.

For HA configuration instructions, visit the High Availability page.
10.3 Switch LAGG

ix2 and ix3 (switch uplink ports 9 and 10), are configured as a load-balanced LAGG. This provides an aggregate uplink capable of 5Gbps for ethernet switchports ETH1-8. This is further demonstrated in the diagram below:

When data is received on ETH1-8, the switch is capable of utilizing LAGG to determine whether that data should be sent out of PORT 9 or PORT 10. That data then passes over one of two 2.5Gbps switch links (PORT 9/10) to the SoC. Data coming from PORT 9 has a direct line to ix2 and data from PORT 10 has a direct line to ix3.

pfSense® LAGG will then take in traffic from both ix2 and ix3 as though it came in on a single interface, lagg0. The same concept applies to traffic sourcing from the pfSense LAGG to the switch LAGG.

10.4 Switch VLANs

By default, ETH1 on the switch is configured as a WAN interface and ETH2-8 are configured as the LAN interface. These eight switchports are customizable and each can be configured to act as an independent interface. For example, all of these configurations are possible:

- ETH1-8 dedicated as a LAN switch
- ETH1-4 configured as a switch for LAN network A and ETH5-8 configured as a switch for LAN network B
- ETH1-8 configured as individual network interfaces
- ETH1 configured for WAN A, ETH2 configured for WAN B, ETH3 configured for LAN network A, ETH4-6 configured as a switch for LAN network B, and ETH8 configured as a H/A sync port.

These scenarios are possible by utilizing VLANs. Each of the switchports (ETH1-8 and POR9-10) are VLAN aware interfaces. They are capable of functioning like a standard access or trunk port:

Access Port: Adds a VLAN tag to inbound untagged traffic
Trunk Port: Allows tagged traffic containing specified VLAN IDs

In the default configuration, two VLANs are used to create the ETH1 WAN interface and ETH2-8 LAN interface:
ETH1-8 are configured to act as **Access** ports.

- When data comes into the ETH1 interface, a VLAN tag of 4090 is added to the ethernet frame.
- When data comes into interfaces ETH2-8, a VLAN tag of 4091 is added to the ethernet frame.

PORT9-10 are configured to act as **Trunk** ports.

- By default, only ethernet frames containing a VLAN tag of 4090 or 4091 are allowed over the trunk.

Each VLAN configured on the switch uses the LAGG interface as its parent interface. For example, the default interface assignment for WAN and LAN:

<table>
<thead>
<tr>
<th>Interface</th>
<th>VLAN Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN</td>
<td>lagg0.4090</td>
</tr>
<tr>
<td>LAN</td>
<td>lagg0.4091</td>
</tr>
</tbody>
</table>

This means **vlan4090** and **vlan4091**, as well as any other VLANs created for the switch, all share the same 5Gbps LAGG uplink across two 2.5Gbps links. The visual below demonstrates how the VLAN tagging works along with the traffic flow:

![VLAN Tagging Diagram](image)

**Note:** Traffic leaving and entering the ETH1-3 interfaces in the visual above are untagged. Devices sending/receiving traffic over these ports do not need to be VLAN aware. The VLAN tagging that occurs within the switch is completely transparent to clients. It’s used solely for segmenting switch traffic internally.

Aside from being able to specify whether a switchport should act as an access or trunk port, it’s also possible to disable 802.1q VLAN mode. When this is done, a third mode called **Port VLAN Mode** is enabled. In this mode, any and all VLAN tags are allowed on all ports. No VLAN tags are added or removed. Think of it as a dummy switch that retains VLAN tags on frames, if present. This mode is useful when you have numerous VLANs on your network and want to physically segment the switch, while allowing the same VLANs on all segments of the switch.

In **Port VLAN Mode**, rather than specifying which interfaces are associated to a VLAN, you can specify which physical ports form a switch. For example, if I want to create two physical switches that act as individual dummy switches - allowing tagged or untagged traffic, I could configure **Port VLAN Mode** like so:

```plaintext
// UPLINKS
VLAN group 9, Port 9, Members 1,2,3,4,10
VLAN group 10, Port 10, Members 1,2,3,4,9

// SWITCH-A
VLAN group 1, Port 1, Members 2,3,4,9,10
VLAN group 2, Port 2, Members 1,3,4,9,10
VLAN group 3, Port 3, Members 1,2,4,9,10
VLAN group 4, Port 4, Members 1,2,3,9,10
```

(continues on next page)
With this configuration in place, ETH1-8 now function like so:

```
// SWITCH-A
PORT 1 = ETH1
PORT 2 = ETH2
PORT 3 = ETH3
PORT 4 = ETH4
PORT 9 = UPLINK 1
PORT 10 = UPLINK 2

// SWITCH-B
PORT 5 = ETH5
PORT 6 = ETH6
PORT 7 = ETH7
PORT 8 = ETH8
```

**SWITCH-A**

ETH1-4 can talk to each other and to the LAGG uplink. PORT9-10 are members of this switch…this is required for this switch to have uplink to pfSense.

**SWITCH-B**

ETH5-8 can talk to each other but because PORT9-10 are not included as members, clients connecting to ETH5-8 can only talk to other clients on ETH5-8. They will not be able to reach the SoC where ix2 and ix3 are defined, so they never reach pfSense. This can be useful if you want a device other than pfSense to act as the primary uplink for those connected clients.

Since WAN and LAN are assigned to lag0.4090 and lag0.4091, if Port VLAN Mode is enabled, be sure to update the LAN and WAN interface assignment to reference the appropriate VLAN. Also remember to create the new VLANs with lag0 as the parent interface.

If Port VLAN Mode is being used to handle untagged traffic, the LAGG0 interface should be added, enabled, and configured under Interface Assignments.

See also:

For more information on how to configure the switch ports, see *Configuring the Switch Ports.*
11.1 Netgate Training

Netgate training offers training courses for increasing your knowledge of pfSense® 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

11.2 Resource Library

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

https://www.netgate.com/resources

11.3 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®. These items are offered as professional services and can be purchased and scheduled accordingly.

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

11.4 Community Options

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

https://forum.netgate.com/
CHAPTER TWELVE

WARRANTY AND SUPPORT

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

For support information, view our support plans.

See also:

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