CONTENTS

1 Out of the Box 2
2 How-To Guides 20
3 References 35
This Quick Start Guide covers the first time connection procedures for the Netgate® SG-2440 Firewall Appliance and will provide the information needed to keep the appliance up and running.
1.1 Getting Started

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 into 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.

### 1.1.1 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.

### 1.1.2 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

### 1.1.3 Wizard

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

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 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`.

1.1.6 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 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.

### 1.1.8 Time Server Configuration

![Time Server Information](image)

- **Time server hostname**: 0.pfsense.pool.ntp.org
- **Timezone**: America/Chicago

Click **Next** after filling in the fields as appropriate.

### 1.1.9 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.

### 1.1.10 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](image)

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

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.

### 1.1.13 Configuring MTU and MSS

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

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

<table>
<thead>
<tr>
<th>PPPoE configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPPoE Username</td>
</tr>
<tr>
<td>PPPoE Password</td>
</tr>
<tr>
<td>Show PPPoE password</td>
</tr>
<tr>
<td>Reveal password characters</td>
</tr>
<tr>
<td>PPPoE Service name</td>
</tr>
<tr>
<td>Hint: this field can usually be left empty</td>
</tr>
<tr>
<td>PPPoE Dial on demand</td>
</tr>
<tr>
<td>Enable Dial-On-Demand mode</td>
</tr>
<tr>
<td>PPPoE Idle timeout</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>RFC1918 Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block RFC1918 Private Networks</td>
</tr>
<tr>
<td>When set, this option blocks traffic from IP addresses that are reserved for private networks 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Block bogon networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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.

### 1.1.17 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.
1.1.18 Change Administrator Password

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

1.1.19 Save Changes

Click Reload to save configuration.

1.1.20 Basic Firewall Configured

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

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 your pfSense appliance, sign up for a pfSense Training course or browse our extensive Resource Library.

1.2 Input and Output Ports

![Input and Output Ports Diagram](image)

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Port Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Mini-USB Serial Port</td>
<td>6) OPT1 (igb2)</td>
</tr>
<tr>
<td>2) USB0 (USB 2.0)</td>
<td>7) OPT2 (igb3)</td>
</tr>
<tr>
<td>3) USB1 (USB 2.0)</td>
<td>8) Reset Button</td>
</tr>
<tr>
<td>4) WAN (igb0)</td>
<td>9) SATA Activity / Power Indicator</td>
</tr>
<tr>
<td>5) LAN (igb1)</td>
<td>10) Power Input</td>
</tr>
</tbody>
</table>

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

Note: The rubber caps across the top are antenna ports for available wireless options.

The SG-2440 supports four 1000/100/10Base-T Ethernet ports, connected to the CPU’s on-chip Intel i354 Gbps MACs through a Marvell 88E1543 quad SGMII/PHY. Each RJ-45 has built-in LEDs with the following configuration.

<table>
<thead>
<tr>
<th>Left LED</th>
<th>Right LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green = Link</td>
<td>Amber = 1 Gbps</td>
</tr>
<tr>
<td>Blink = Activity</td>
<td>Green = 100 Mbps</td>
</tr>
<tr>
<td>Off = 10 Mbps</td>
<td>Off = 10 Mbps</td>
</tr>
</tbody>
</table>
1.3 Safety and Legal

1.3.1 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.

1.3.2 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.

1.3.3 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.

1.3.4 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.

1.3.5 Australia and New Zealand

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

1.3.6 CE Marking

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

1.3.7 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


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 deshacerse 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 deshacer 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.

1.3.8 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)

Ελληνικ [Greek]

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

Magyar [Hungarian]

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

Íslenska [Icelandic]

Hér me l 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 citem ar to saist tajiem noteikumiem.

Lietuviškai [Lithuanian]

NETGATE deklaruoja, kad šis NETGATE įrenginys atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
1.3.9 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.

1.3.10 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.

1.3.11 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.

1.3.12 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.

1.3.13 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 THE 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.
2.1 Connecting to the Console Port

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.

2.1.1 Install the Driver

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

If needed, install an appropriate Silicon Labs CP210x USB to UART Bridge driver on the workstation used to connect with the system.

Windows

There are drivers available for Windows available for download.

Mac OSX

There are drivers available for Mac OSX available for download.

For Mac, choose the Macintosh OSX download.

Linux

There are drivers available for Linux available for download.

FreeBSD

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

2.1.2 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.
2.1.3 Locate the Console Port Device

The appropriate console port device that the workstation assigned as the serial port must be located before attempting to connect to the console.

Note: Even if the serial port was assigned in the BIOS, the workstation’s OS may remap it to a different COM Port.

Windows

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

Mac OSX

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/cuU0. Look for messages about the device attaching in the system log files or by running dmesg.

### 2.1.4 Launch a Terminal Program

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

**Windows**

For Windows it is recommended to run PuTTY or SecureCRT. An example of how to configure PuTTY is below.

```
Warning: Do not use Hyperterminal.
```

**Mac OSX**

For Mac OSX it is recommended to run screen, or cu. An example of how to configure screen is below.

**Linux**

For Linux it is recommended to run screen, PuTTY, minicom, or dterm. An example of how to configure PuTTY and screen is below.

**FreeBSD**

For FreeBSD it is recommended to run screen or cu. An example of how to configure screen is below.

### Client-Specific Examples

**PuTTY**

Open PuTTY and select Session under Category on the left hand side. Next, set the Connection type to Serial. Then, set Serial line to the console port that was located above, in Locate the Console Port Device, and the Speed to 115200 bits per second.

Click the Open button and the console screen will be displayed.

**GNU screen**

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

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

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

```
sudo screen -U <console-port> 115200
```
Fig. 1: An example of using PuTTY in Windows.
Terminal Settings

The settings to use within the terminal program are:

- **Speed**: 115200 baud, the speed of the BIOS
- **Data bits**: 8
- **Parity**: none
- **Stop bits**: 1
- **Flow Control**: Off or XON/OFF. Hardware flow control (RTS/CTS) must be disabled.

2.1.5 Troubleshooting

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.

PuTTY has issues with line drawing

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

- **Window Columns x Rows** = 80x24
- **Window > Appearance Font** = *Courier New 10pt* or *Consolas 10pt*
- **Window > Translation Remote Character Set** = *Use font encoding* or *UTF-8*
- **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

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**)
- Ensure the terminal program is configured for the proper character encoding, such as **UTF-8** or **Latin-1**, depending on the operating system. (See **GNU Screen**)

© Copyright 2020 Rubicon Communications LLC
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)
- 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.

2.2 Reinstalling pfSense Software

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 SG-2440 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:

   ```plaintext
   pfSense-netgate-memstick-ADI-2.4.5-RELEASE-amd64.img.gz
   ```

   **Note:** The pfSense® factory version is the version that is preinstalled on Netgate appliances. 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`, which should work for most. Choose the correct console output for your system.

   ```plaintext
   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.

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 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 `bufdaemon` to stop... done
Waiting (max 60 seconds) for system process `syncer` to stop...
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.

### 2.3 mSATA Installation

The SG-2440 has built-in onboard eMMC storage. Optionally, a mSATA drive could 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 mSATA drive will be the first drive recognized by pfSense® software. pfSense must be reinstalled on the mSATA drive.

The mSATA slot is located on the top of the SG-2440 system board. The mSATA slot is directly behind the Ethernet ports. There are two other similar ports on the top of the board, but they are mPCIe ports. The mSATA drives are not electrically compatible with mPCIe connectors.

1. Remove the four (4) case screws, two (2) on each side of the case.
Fig. 3: Case Screws

**Warning:** Many of our desktop systems use tri-lobe self-threading screws. Only use a hand screwdriver and be very careful when screwing them back in. They are very easy to crossthread and will strip the threads of the case.

2. Remove the lid from the base of the chassis.
3. Remove the screws from the mSATA standoffs.
4. Insert the gold leads of the mSATA 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.

5. Push the mSATA drive down until it is parallel with the system board and replace the screws to secure the mSATA drive in place.
6. Replace the lid and case screws. Use a hand screwdriver and be careful not to crossthread the screws.
7. Reinstall the pfSense software on the new mSATA drive.
8. Restore your configuration backup if you have one.

### 2.4 BIOS Flash Procedure

#### 2.4.1 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.
Fig. 4: SG-2440 Open
Fig. 5: Remove the mSATA Standoff Screws
Fig. 6: mSATA Drive Properly Inserted into the Slot
Fig. 7: Secure the mSATA Drive
Fig. 8: mSATA Drive Installed
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.
3.1 Additional Resources

3.1.1 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

3.1.2 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

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®. 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

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/

3.2 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.