## Tested Platforms

1. Tested Platforms

## Untested Platforms

2. Untested Platforms
TNSR software is available pre-installed on Netgate hardware or as a Bare Metal Image (BMI) for use on Commercial Off the Self (COTS) hardware or in virtual environments. For quotes, updates, and more information about TNSR, please visit tnsr.com or contact TNSR sales.

**General System Requirements**

- 64-bit x86 processor with SSE4.2 extensions
- Minimum of 4GB RAM for basic routing functionality
  
  RAM requirements increase significantly if the installation will need to handle large volumes of connections, large volumes of routing data (e.g. full BGP feeds), or multiple worker threads.

  **See also:**

  See Memory Usage and Tuning for information on how to determine optimal memory sizes based on what the router must handle.

- Minimum of 20GB Storage
- Minimum of two network interface ports, three network interface ports recommended (two for dataplane, one for management)
- Option to disable Secure Boot if using UEFI, as it is incompatible with the TNSR dataplane

**Compatibility**

TNSR is a platform for high-speed packet processing, delivered as services that run on top of an operating system. TNSR 21.11 and later are based on Ubuntu, currently the 20.04 LTS release for x86 processors. This platform has been tested by Netgate, so that means most compatibility questions can be resolved by checking whether the hardware can run Ubuntu Linux 20.04.

- **Tested Platforms**
- **Untested Platforms**
CHAPTER ONE

TESTED PLATFORMS

These systems and components have been tested extensively by Netgate and are known to work well with TNSR. In addition to the support included with the TNSR license, Netgate warranty and technical support is available for purchase for Netgate-branded appliances.

1.1 Netgate Appliances

- Netgate 5100
- Netgate 6100 MAX
- Netgate 8200
- Netgate 1537-1U
- Netgate 1541-1U

1.1.1 Netgate 5100 Secure Router Manual

This Quick Start Guide covers the first time connection procedures for the Netgate 5100 Secure Router and also provides information needed to stay up and running.
Getting Started

Use the following steps to configure the TNSR Secure Router.

1. To configure the Network Interfaces and gaining access to the Internet, follow the instructions provided in the Zero-to-Ping documentation.

   **Note:** Not all steps in the Zero-to-Ping documentation will be necessary for every configuration scenario.

2. Once the Host OS is capable of reaching the Internet, check for updates (Updating TNSR) before proceeding. This ensures the security and integrity of the router before TNSR interfaces are exposed to the Internet.

3. Finally, configure the TNSR instance to meet the specific use case. The topics are listed on the left column of the TNSR Documentation site. There are also TNSR Configuration Example Recipes that might be of assistance when configuring TNSR.

Input and Output Ports

Rear Side

![Netgate 5100 Network Interface Layout](image)

Network Ports

<table>
<thead>
<tr>
<th>Port Label</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGB0</td>
<td>enp3s0</td>
<td>GigabitEthernet3/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>IGB1</td>
<td>enp4s0</td>
<td>GigabitEthernet4/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>IX0</td>
<td>enp6s0f0</td>
<td>GigabitEthernet6/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>IX1</td>
<td>enp6s0f1</td>
<td>GigabitEthernet6/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>IX2</td>
<td>enp8s0f0</td>
<td>GigabitEthernet8/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>IX3</td>
<td>enp8s0f1</td>
<td>GigabitEthernet8/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is `enp3s0`. The Host OS Interface is one network interface that is only available to
the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

<table>
<thead>
<tr>
<th>Status LED</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left LED</td>
<td>Solid Amber</td>
<td>Link has been established and there is no activity on this port</td>
</tr>
<tr>
<td>(Link Status)</td>
<td>Blinking Amber</td>
<td>Link has been established and there is activity on this port</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No link has been established</td>
</tr>
<tr>
<td>Right LED</td>
<td>Solid Green</td>
<td>Operating as a 100 Mbps connection</td>
</tr>
<tr>
<td>(Speed)</td>
<td>Blinking Amber</td>
<td>Operating as a Gigabit connection (1000 Mbps)</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No link has been established</td>
</tr>
</tbody>
</table>

**Other Ports and Indicators**

- Console (Mini-USB)
- Status LEDs
- 2x USB 3.0

**Front Side**

1. Recessed Reset Button
2. Power Button
3. Power (12VDC with threaded locking connector)

*Note:* The power button on the Netgate 5100 has been programmed to perform a graceful shutdown when depressed.
Connecting to the Console Port

This guide shows how to access the serial console which can be used for troubleshooting and diagnostics tasks as well as some basic configuration.

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

Install the Driver

A Prolific PL2303 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 Prolific PL2303 USB to UART Bridge driver on the workstation used to connect with the device.

Windows

There are drivers available for Windows available for download.

macOS

There are drivers available for macOS available for download.

Linux

There are drivers available for Linux available for download.

FreeBSD

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 device side completely. With most cables there will be a tangible “click”, “snap”, or similar indication when the cable is fully engaged.
Apply Power to the Device

On some devices when using a USB serial console port the serial port will not appear on the client operating system until the device is plugged into a power source.

If the client OS does not see the serial device, connect the power cord to the device to allow it to start booting.

If the device appears without power, then better to wait until the terminal is open before connecting power so the client can view the entire boot output.

Locate the Console Port Device

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

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

Windows

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

macOS

The device associated with the system console is likely to show up as, or start with, /dev/cu.usbserial-<id>.
Run `ls -l /dev/cu.*` from a Terminal prompt to see a list of available USB serial devices and locate the appropriate one for the hardware. If there are multiple devices, the correct device is likely the one with the most recent timestamp or highest ID.

**Linux**

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

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

**FreeBSD**

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

**Note:** If the serial device is not present, ensure the device has power and then check again.

### Launch a Terminal Program

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

**Windows**

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

**Warning:** Do not use **Hyperterminal**.

**macOS**

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

**Linux**

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

**FreeBSD**

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

### Client-Specific Examples

**PuTTY in Windows**

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

1.1. Netgate Appliances
• Click the Open button
PuTTY will then display the console.

![PuTTY Configuration](image)

**Fig. 1: An example of using PuTTY in Windows**

**PuTTY in Linux**

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

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

• Set the **Connection type** to **Serial**
• Set **Serial line** to `/dev/ttyUSB0`
• Set the **Speed** to 115200 bits per second
• Click the Open button
PuTTY will then display the console.
GNU screen

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

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

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

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

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

The settings to use within the terminal program are:

**Speed**
- 115200 baud, the speed of the BIOS

**Data bits**
- 8

**Parity**
- None

**Stop bits**
- 1

**Flow Control**
- Off or XON/OFF.

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

What’s Next?

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

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

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

Troubleshooting

Serial Device Missing

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

**No Power**
- Some models require power before the client can connect to the USB serial console.

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

**Bad USB Cable**
- Some USB cables are not suitable for use as data cables. For example, some cables are only capable of delivering power for charging devices and not acting as data cables. Others may be of low quality or have poor or worn connectors.
- The ideal cable to use is the one that came with the device. Failing that, ensure the cable is of the correct type and specifications, and try multiple cables.

**Wrong Device**
- In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.
Hardware Failure
There could be a hardware failure preventing the serial console from working. Contact Netgate TAC for assistance.

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

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

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

Wrong Terminal Settings
Ensure the terminal program is configured for the correct speed. The default BIOS speed is 115200, and many other modern operating systems use that speed as well.
Some older operating systems or custom configurations may use slower speeds such as 9600 or 38400.

Device OS Serial Console Settings
Ensure the operating system is configured for the proper console (e.g. ttyS1 in Linux). Consult the various operating install guides on this site for further information.

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

Window
Columns x Rows
80x24

Window > Appearance
Font
Courier New 10pt or Consolas 10pt

Window > Translation
Remote Character Set
Use font encoding or UTF-8
Handling of line drawing characters
Use font in both ANSI and OEM modes or Use Unicode line drawing code points

Window > Colours
Indicate bolded text by changing
The colour
Garbled Serial Output

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

Flow Control
In some cases flow control can interfere with serial communication, causing dropped characters or other issues. Disabling flow control in the client can potentially correct this problem.

On PuTTY and other GUI clients there is typically a per-session option to disable flow control. In PuTTY, the Flow Control option is in the settings tree under Connection, then Serial.

To disable flow control in GNU Screen, add the `-ixon` and/or `-ixoff` parameters after the serial speed as in the following example:

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

Terminal Speed
Ensure the terminal program is configured for the correct speed. (See No Serial Output)

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

Serial Output Stops After the BIOS

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

Terminal Speed
Ensure the terminal program is configured for the correct speed for the installed operating system. (See No Serial Output)

Device OS Serial Console Settings
Ensure the installed operating system is configured to activate the serial console and that it is configured for the proper console (e.g. `ttyS1` in Linux). Consult the various operating install guides on this site for further information.

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

Additional Resources

Professional Services

Support does not cover more complex tasks such as network design and conversion from other firewalls. These items are offered as professional services and can be purchased and scheduled accordingly.

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

Netgate training offers training courses for increasing your knowledge of Netgate 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/

Resource Library

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

https://www.netgate.com/resources/

Warranty and Support

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

Enterprise Support is included with an active software subscription, for more information view the Netgate Global Support page.

See also:

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

1.1.2 Netgate 6100 MAX Secure Router Manual

This Quick Start Guide covers the first time connection procedures for the Netgate 6100 MAX Secure Router and also provides information needed to stay up and running.
Getting Started

Use the following steps to configure the TNSR Secure Router.

1. To configure the Network Interfaces and gaining access to the Internet, follow the instructions provided in the Zero-to-Ping documentation.

   **Note:** Not all steps in the Zero-to-Ping documentation will be necessary for every configuration scenario.

2. Once the Host OS is capable of reaching the Internet, check for updates (Updating TNSR) before proceeding. This ensures the security and integrity of the router before TNSR interfaces are exposed to the Internet.

3. Finally, configure the TNSR instance to meet the specific use case. The topics are listed on the left column of the TNSR Documentation site. There are also TNSR Configuration Example Recipes that might be of assistance when configuring TNSR.

Input and Output Ports

![Rear view of the Netgate 6100 MAX Secure Router](image)

*Fig. 3: Rear view of the Netgate 6100 MAX Secure Router*

The numbered labels in this image refer to entries in Networking Ports and Other Ports.

Networking Ports

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

**Note:** Each port, WAN1 and WAN2, is discrete and individual. It is possible to use the RJ-45 connector on one port and the SFP connector on the other.
Table 2: Netgate 6100 Network Interface Layout

<table>
<thead>
<tr>
<th>Port</th>
<th>Label</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>WAN1</td>
<td>enp2s0f1</td>
<td>GigabitEthernet2/0/1</td>
<td>RJ-45/SFP</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>WAN2</td>
<td>enp2s0f0</td>
<td>GigabitEthernet2/0/0</td>
<td>RJ-45/SFP</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>WAN3</td>
<td>enp3s0f0</td>
<td>TenGigabitEthernet3/0/0</td>
<td>SFP</td>
<td>1/10 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>WAN4</td>
<td>enp3s0f1</td>
<td>TenGigabitEthernet3/0/1</td>
<td>SFP</td>
<td>1/10 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>LAN1</td>
<td>enp4s0</td>
<td>TwoDotFiveGigabitEthernet4/0/0</td>
<td>RJ-45</td>
<td>2.5 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>LAN2</td>
<td>enp5s0</td>
<td>TwoDotFiveGigabitEthernet5/0/0</td>
<td>RJ-45</td>
<td>2.5 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>LAN3</td>
<td>enp6s0</td>
<td>TwoDotFiveGigabitEthernet6/0/0</td>
<td>RJ-45</td>
<td>2.5 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>LAN4</td>
<td>enp7s0</td>
<td>TwoDotFiveGigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>2.5 Gbps</td>
</tr>
</tbody>
</table>

**Note:** The default Host OS Interface is enp2s0f0. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

**SFP+ Ethernet Ports**

WAN3 and WAN4 are discrete ports, each with dedicated 10 Gbps back to the Intel SoC.

**Warning:** The built-in SFP interfaces on C3000 systems do not support modules utilizing copper Ethernet connectors (RJ45). As such, copper SFP/SFP+ modules are not supported on this platform.

**Note:** Intel notes the following additional limitations on these interfaces:

Devices based on the Intel(R) Ethernet Connection X552 and Intel(R) Ethernet Connection X553 do not support the following features:

- Energy Efficient Ethernet (EEE)
- Intel PROSet for Windows Device Manager
- Intel ANS teams or VLANs (LBFO is supported)
- Fibre Channel over Ethernet (FCoE)
- Data Center Bridging (DCB)
- IPSec Offloading
- MACSec Offloading

In addition, SFP+ devices based on the Intel(R) Ethernet Connection X552 and Intel(R) Ethernet Connection X553 do not support the following features:

- Speed and duplex auto-negotiation.
- Wake on LAN
- 1000BASE-T SFP Modules

1.1. Netgate Appliances
Other Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Serial Console</td>
</tr>
<tr>
<td>6</td>
<td>Power</td>
</tr>
</tbody>
</table>

- Clients can access the *Serial Console* using either the built in serial interface with a Micro-USB B cable or an RJ45 “Cisco” style cable and separate serial adapter.

**Note:** Only one type of console connection will work at a time and the RJ45 console connection has priority. If both ports are connected only the RJ45 console port will function.

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

Front Side

![Fig. 4: Front view of the Netgate 6100 Firewall Appliance](image)

LED Patterns

<table>
<thead>
<tr>
<th>Description</th>
<th>LED Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standby</td>
<td>Circle solid orange</td>
</tr>
<tr>
<td>Power On</td>
<td>Circle solid blue</td>
</tr>
</tbody>
</table>
Left Side

![Netgate 6100 Firewall Appliance](image)

Fig. 5: Left side view of the Netgate 6100 Firewall Appliance

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

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reset Button (Recessed)</td>
<td>No function on TNSR at this time</td>
</tr>
<tr>
<td>2</td>
<td>Power Button (Protruding)</td>
<td>Short Press (Hold 3-5s) Graceful shutdown, Power on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Long Press (Hold 7-12s) Hard power cut to CPU</td>
</tr>
<tr>
<td>3</td>
<td>2x USB 3.0 Ports</td>
<td>Connect USB Devices</td>
</tr>
</tbody>
</table>

Connecting to the Console Port

This guide shows how to access the serial console which can be used for troubleshooting and diagnostics tasks as well as some basic configuration.

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

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 Micro-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 device.

Windows

There are drivers available for Windows available for download.

macOS

There are drivers available for macOS available for download.

For macOS, choose the CP210x VCP Mac download.

Linux

There are drivers available for Linux available for download.

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

**Connect a USB Cable**

Next, locate an appropriate USB cable that has a **USB Micro-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 Micro-B (5-pin)** plug end into the console port on the appliance and connect the **USB Type A** plug into an available USB port on the workstation.

---

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

---

**Apply Power to the Device**

On some devices when using a USB serial console port the serial port will not appear on the client operating system until the device is plugged into a power source.

If the client OS does not see the serial device, connect the power cord to the device to allow it to start booting.

If the device appears without power, then better to wait until the terminal is open before connecting power so the client can view the entire boot output.

**Locate the Console Port Device**

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

---

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

---

**Windows**

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

The device associated with the system console is likely to show up as, or start with, /dev/cu.usbserial-*<id>*.

Run `ls -l /dev/cu.*` from a Terminal prompt to see a list of available USB serial devices and locate the appropriate one for the hardware. If there are multiple devices, the correct device is likely the one with the most recent timestamp or highest ID.

Linux

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

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

FreeBSD

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

Note: If the serial device is not present, ensure the device has power and then check again.
Launch a Terminal Program

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

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

**Warning:** Do not use *Hyperterminal*.

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

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

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

Client-Specific Examples

**PuTTY in Windows**

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

PuTTY will then display the console.

**PuTTY in Linux**

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

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

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

PuTTY will then display the console.
Fig. 6: An example of using PuTTY in Windows
GNU screen

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

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

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

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

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

The settings to use within the terminal program are:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>115200 baud, the speed of the BIOS</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow Control</td>
<td>Off or XON/OFF.</td>
</tr>
</tbody>
</table>

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

What's Next?

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

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

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

Troubleshooting

Serial Device Missing

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

No Power
Some models require power before the client can connect to the USB serial console.

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

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

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

Wrong Device
In some cases there may be multiple serial devices available. Ensure the one used by the serial client is the correct one. Some devices expose multiple ports, so using the incorrect port may lead to no output or unexpected output.
Hardware Failure
There could be a hardware failure preventing the serial console from working. Contact Netgate TAC for assistance.

No Serial Output

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

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

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

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

Device OS Serial Console Settings
Ensure the operating system is configured for the proper console (e.g. ttyS1 in Linux). Consult the various operating install guides on this site for further information.

PuTTY has issues with line drawing

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

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

Window

Columns x Rows
80x24

Window > Appearance

Font
Courier New 10pt or Consolas 10pt

Window > Translation

Remote Character Set
Use font encoding or UTF-8

Handling of line drawing characters
Use font in both ANSI and OEM modes or Use Unicode line drawing code points

Window > Colours

Indicate bolded text by changing
The colour
Garbled Serial Output

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

Flow Control
In some cases flow control can interfere with serial communication, causing dropped characters or other issues. Disabling flow control in the client can potentially correct this problem.

On PuTTY and other GUI clients there is typically a per-session option to disable flow control. In PuTTY, the Flow Control option is in the settings tree under Connection, then Serial.

To disable flow control in GNU Screen, add the -ixon and/or -ixooff parameters after the serial speed as in the following example:

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

Terminal Speed
Ensure the terminal program is configured for the correct speed. (See No Serial Output)

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

Serial Output Stops After the BIOS

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

Terminal Speed
Ensure the terminal program is configured for the correct speed for the installed operating system. (See No Serial Output)

Device OS Serial Console Settings
Ensure the installed operating system is configured to activate the serial console and that it is configured for the proper console (e.g. ttyS1 in Linux). Consult the various operating install guides on this site for further information.

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

Additional Resources

Professional Services
Support does not cover more complex tasks such as network design and conversion from other firewalls. These items are offered as professional services and can be purchased and scheduled accordingly.

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

Netgate training offers training courses for increasing your knowledge of Netgate 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/

Resource Library

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

https://www.netgate.com/resources/

Warranty and Support

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

Enterprise Support is included with an active software subscription, for more information view the Netgate Global Support page.

See also:

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

1.1.3 Netgate 8200 Secure Router Manual

This Quick Start Guide covers the first time connection procedures for the Netgate® 8200 Secure Router and also provides information needed to stay up and running.

Hardware Overview

1U Rack Mount Design

The Netgate 8200 Secure Router was designed with rack mounting in mind and comes pre-assembled in a 1U rack mount configuration. The device can safely be mounted directly above another device in a rack, such as for an HA configuration.
Fig. 8: Netgate 8200 Secure Router Front Angled View

Fig. 9: Netgate 8200 Secure Router HA Pair – Front View
**Note:** Parts are included in the box to convert it into a desktop configuration, but this guide assumes the device remains in its rack mount configuration.

---

### Active Cooling

The Netgate 8200 Secure Router has an actively controlled cooling fan integrated into the chassis baseplate. The fan automatically adjusts its speed based on the temperature of the device, which allows the unit to remain uncharacteristically quiet for such a powerful 1U system.

![Netgate 8200 Secure Router – Bottom View](image)

**Fig. 10: Netgate 8200 Secure Router – Bottom View**

**Note:** The fan will continue to run at a low idle speed of 560 RPM when the Netgate 8200 is powered off. Components may still be hot for some time after shutdown and the airflow from the fan brings their temperature down. The fan will stop if the CPU temperature falls below 5C (41F).

**Warning:** Do not block the portion of the fan intake under the network ports. The bottom of the unit can be placed on top of another device so long as the fan intake under the network ports can pull in air unobstructed.
Available Storage

The Netgate 8200 Secure Router is available only in a MAX style configuration with an NVMe SSD for storage. This model does not have built-in eMMC storage.

Getting Started

Use the following steps to configure the TNSR Secure Router.

1. To configure the Network Interfaces and gaining access to the Internet, follow the instructions provided in the Zero-to-Ping documentation.

   Note: Not all steps in the Zero-to-Ping documentation will be necessary for every configuration scenario.

2. Once the Host OS is capable of reaching the Internet, check for updates (Updating TNSR) before proceeding. This ensures the security and integrity of the router before TNSR interfaces are exposed to the Internet.

3. Finally, configure the TNSR instance to meet the specific use case. The topics are listed on the left column of the TNSR Documentation site. There are also TNSR Configuration Example Recipes that might be of assistance when configuring TNSR.

Input and Output Ports

Fig. 11: Front view of the Netgate 8200 Secure Router ports

The numbered labels in this image refer to entries in Networking Ports and Non-Networking Ports.

Non-Networking Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Serial Console</td>
</tr>
<tr>
<td>6</td>
<td>Power</td>
</tr>
<tr>
<td>7</td>
<td>Fan intake (Do not block)</td>
</tr>
</tbody>
</table>

- Clients can access the Serial Console using either the built in serial interface with a Micro-USB B cable or an RJ45 “Cisco” style cable and separate serial adapter.

   Note: Only one type of console connection will work at a time and the RJ45 console connection has priority. If both ports are connected only the RJ45 console port will function.

- The Power connector is 12VDC with threaded locking connector. Power Consumption 20W (idle)
The Netgate 8200 Secure Router is actively cooled by a fan located on the bottom of the device as mentioned in Active Cooling. The portion of the fan intake under the networking ports is where it draws in air when mounted against another device. Do not block this part of the air intake.

Networking Ports

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

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Label</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>WAN1</td>
<td>enp2s0f1</td>
<td>GigabitEthernet2/0/1</td>
<td>RJ-45/SFP</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>WAN2</td>
<td>enp2s0f0</td>
<td>GigabitEthernet2/0/0</td>
<td>RJ-45/SFP</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>WAN3</td>
<td>enp3s0f0</td>
<td>TenGigabitEthernet3/0/0</td>
<td>SFP</td>
<td>1/10 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>WAN4</td>
<td>enp3s0f1</td>
<td>TenGigabitEthernet3/0/1</td>
<td>SFP</td>
<td>1/10 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>LAN1</td>
<td>enp4s0</td>
<td>TwoDotFiveGigabitEthernet4/0/0</td>
<td>RJ-45</td>
<td>2.5 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>LAN2</td>
<td>enp5s0</td>
<td>TwoDotFiveGigabitEthernet5/0/0</td>
<td>RJ-45</td>
<td>2.5 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>LAN3</td>
<td>enp6s0</td>
<td>TwoDotFiveGigabitEthernet6/0/0</td>
<td>RJ-45</td>
<td>2.5 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>LAN4</td>
<td>enp7s0</td>
<td>TwoDotFiveGigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>2.5 Gbps</td>
</tr>
</tbody>
</table>

Note: The default Host OS Interface is enp2s0f0. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

SFP+ Ethernet Ports

WAN3 and WAN4 are discrete ports, each with dedicated 10 Gbps back to the Intel SoC.

Warning: The built-in SFP interfaces on C3000 systems do not support modules utilizing copper Ethernet connectors (RJ45). As such, copper SFP/SFP+ modules are not supported on this platform.

Note: Intel notes the following additional limitations on these interfaces:

Devices based on the Intel(R) Ethernet Connection X552 and Intel(R) Ethernet Connection X553 do not support the following features:

- Energy Efficient Ethernet (EEE)
- Intel PROSet for Windows Device Manager
- Intel ANS teams or VLANs (LBFO is supported)
- Fibre Channel over Ethernet (FCoE)
- Data Center Bridging (DCB)
• IPSec Offloading
• MACSec Offloading

In addition, SFP+ devices based on the Intel(R) Ethernet Connection X552 and Intel(R) Ethernet Connection X553 do not support the following features:

• Speed and duplex auto-negotiation.
• Wake on LAN
• 1000BASE-T SFP Modules

---

**Rear Side**

Fig. 12: Rear view of the Netgate 8200 Secure Router
LED Patterns

<table>
<thead>
<tr>
<th>Description</th>
<th>LED Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standby</td>
<td>Circle solid orange</td>
</tr>
<tr>
<td>Power On</td>
<td>Circle solid blue</td>
</tr>
</tbody>
</table>

Right Side

Fig. 13: Right side view of the Netgate 8200 Secure Router

The right side panel of the device (when facing the front of the 1U rack mount) contains:

<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reset Button (Recessed)</td>
<td>No function on TNSR at this time</td>
</tr>
<tr>
<td>2</td>
<td>Power Button (Protruding)</td>
<td>Short Press (Hold 3-5s) Graceful shutdown, Power on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Long Press (Hold 7-12s) Hard power cut to CPU</td>
</tr>
<tr>
<td>3</td>
<td>2x USB 3.0 Ports</td>
<td>Connect USB Devices – Extended to USB ports on the rack mount</td>
</tr>
</tbody>
</table>

Fig. 14: Netgate 8200 Secure Router Front View – USB Ports on the Right
Connecting to the Console Port

This guide shows how to access the serial console which can be used for troubleshooting and diagnostics tasks as well as some basic configuration.

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

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 Micro-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 device.

Windows

There are drivers available for Windows available for download.

macOS

There are drivers available for macOS available for download.

For macOS, choose the CP210x VCP Mac download.

Linux

There are drivers available for Linux available for download.

FreeBSD

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

Connect a USB Cable

Next, locate an appropriate USB cable that has a USB Micro-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 Micro-B (5-pin) plug end into the console port on the appliance and connect the USB Type A plug into an available USB port on the workstation.

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

On some devices when using a USB serial console port the serial port will not appear on the client operating system until the device is plugged into a power source.

If the client OS does not see the serial device, connect the power cord to the device to allow it to start booting.

If the device appears without power, then better to wait until the terminal is open before connecting power so the client can view the entire boot output.

Locate the Console Port Device

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

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

Windows

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

The device associated with the system console is likely to show up as, or start with, /dev/cu.usbserial-<id>.

Run `ls -l /dev/cu.*` from a Terminal prompt to see a list of available USB serial devices and locate the appropriate one for the hardware. If there are multiple devices, the correct device is likely the one with the most recent timestamp or highest ID.

Linux

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

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

FreeBSD

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

**Note:** If the serial device is not present, ensure the device has power and then check again.

### Launch a Terminal Program

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

**Windows**

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

**Warning:** Do not use *Hyperterminal*.

**macOS**

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

**Linux**

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

**FreeBSD**

For FreeBSD the best practice is to run GNU *screen* or *cu*. An example of how to configure GNU *screen* is below.
Client-Specific Examples

PuTTY in Windows

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

PuTTY will then display the console.

![PuTTY Configuration](image)

Fig. 15: An example of using PuTTY in Windows
PuTTY in Linux

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

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

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

PuTTY will then display the console.

![PuTTY Configuration](image)

Fig. 16: An example of using PuTTY in Linux

**GNU screen**

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

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

**Note:** The `sudo` command will prompt for the local workstation password of the current account.
If portions of the text are unreadable but appear to be properly formatted, the most likely culprit is a character encoding mismatch in the terminal. Adding the `-U` parameter to the `screen` command line arguments forces it to use UTF-8 for character encoding:

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

**Terminal Settings**

The settings to use within the terminal program are:

- **Speed**
  - 115200 baud, the speed of the BIOS
- **Data bits**
  - 8
- **Parity**
  - None
- **Stop bits**
  - 1
- **Flow Control**
  - Off or XON/OFF.

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

**What's Next?**

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

- If the device does not yet have power applied, plug it in and monitor the terminal output.
- If the device is already powered on, try pressing `Space`. If there is still no output, press `Enter`. If the device was booted, it should redisplay the login prompt or produce other output indicating its status.

**Troubleshooting**

**Serial Device Missing**

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

- **No Power**
  - Some models require power before the client can connect to the USB serial console.
- **USB Cable Not Plugged In**
  - For USB consoles, the USB cable may not be fully engaged on both ends. Gently, but firmly, ensure the cable has a good connection on both sides.
- **Bad USB Cable**
  - Some USB cables are not suitable for use as data cables. For example, some cables are only capable of delivering
power for charging devices and not acting as data cables. Others may be of low quality or have poor or worn connectors.

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

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

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

No Serial Output

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

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

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

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

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

Device OS Serial Console Settings
Ensure the operating system is configured for the proper console (e.g. ttyS1 in Linux). Consult the various operating install guides on this site for further information.

PuTTY has issues with line drawing

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

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

Window

Columns x Rows
80x24

Window > Appearance

Font
Courier New 10pt or Consolas 10pt

Window > Translation

Remote Character Set
Use font encoding or UTF-8

Handling of line drawing characters
Use font in both ANSI and OEM modes or Use Unicode line drawing code points
Garbled Serial Output

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

**Flow Control**
In some cases flow control can interfere with serial communication, causing dropped characters or other issues. Disabling flow control in the client can potentially correct this problem.

On PuTTY and other GUI clients there is typically a per-session option to disable flow control. In PuTTY, the **Flow Control** option is in the settings tree under **Connection**, then **Serial**.

To disable flow control in GNU Screen, add the `-ixon` and/or `-ixoff` parameters after the serial speed as in the following example:

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

**Terminal Speed**
Ensure the terminal program is configured for the correct speed. (See **No Serial Output**)

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

Serial Output Stops After the BIOS

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

**Terminal Speed**
Ensure the terminal program is configured for the correct speed for the installed operating system. (See **No Serial Output**)

**Device OS Serial Console Settings**
Ensure the installed operating system is configured to activate the serial console and that it is configured for the proper console (e.g. `ttyS1` in Linux). Consult the various operating install guides on this site for further information.

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

Additional Resources

**Professional Services**

Support does not cover more complex tasks such as network design and conversion from other firewalls. These items are offered as professional services and can be purchased and scheduled accordingly.

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

Netgate training offers training courses for increasing your knowledge of Netgate 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/

Resource Library

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

https://www.netgate.com/resources/

Warranty and Support

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

Enterprise Support is included with an active software subscription, for more information view the Netgate Global Support page.

See also:

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

1.1.4 Netgate 1537 Secure Router Manual

This Quick Start Guide covers the first time connection procedures for the Netgate 1537 1U Secure Router and also provides information needed to stay up and running.
Getting Started

Use the following steps to configure the TNSR Secure Router.

1. To configure the Network Interfaces and gaining access to the Internet, follow the instructions provided in the Zero-to-Ping documentation.

   **Note:** Not all steps in the Zero-to-Ping documentation will be necessary for every configuration scenario.

2. Once the Host OS is capable of reaching the Internet, check for updates (Updating TNSR) before proceeding. This ensures the security and integrity of the router before TNSR interfaces are exposed to the Internet.

3. Finally, configure the TNSR instance to meet the specific use case. The topics are listed on the left column of the TNSR Documentation site. There are also TNSR Configuration Example Recipes that might be of assistance when configuring TNSR.

Input and Output Ports

**Contents**

- Input and Output Ports
  - Default Configuration
    - Network Ports
    - Other I/O
    - Status LEDs
  - With CPIC-8955 Accelerator Card with Intel® QuickAssist Technology
  - With 2 Port Intel 1 Gbps Ethernet Expansion Card
  - With 2 Port Intel 10 Gbps X710 SFP+ Expansion Card
  - With 4 Port Intel 1 Gbps Ethernet Expansion Card
  - With 4 Port Intel 10 Gbps X710 SFP+ Expansion Card

Default Configuration

![Diagram of TNSR Secure Router with numbered ports](image-url)
Network Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eno1</td>
<td>GigabitEthernet6/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>eno2</td>
<td>GigabitEthernet6/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>eno3</td>
<td>TenGigabitEthernet3/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>eno4</td>
<td>TenGigabitEthernet3/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

Other I/O

<table>
<thead>
<tr>
<th>Port</th>
<th>I/O Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2x USB 3.0</td>
</tr>
<tr>
<td>6</td>
<td>IPMI</td>
</tr>
<tr>
<td>7</td>
<td>VGA</td>
</tr>
<tr>
<td>8</td>
<td>Reset &amp; Power buttons</td>
</tr>
<tr>
<td>9</td>
<td>Status LEDs (see table below)</td>
</tr>
</tbody>
</table>

Status LEDs

![Status LEDs Image]
<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9a</td>
<td>Continuously on and red</td>
<td>An overheat condition has occurred. (This may be caused by cable congestion.)</td>
</tr>
<tr>
<td></td>
<td>Blinking red (1Hz)</td>
<td>Fan failure, check for an inoperative fan.</td>
</tr>
<tr>
<td></td>
<td>Blinking red (0.25Hz)</td>
<td>Power failure, check for a non-operational power supply.</td>
</tr>
<tr>
<td></td>
<td>Solid blue</td>
<td>Local UID has been activated. Use this function through IPMI to locate the server in a rack mount environment.</td>
</tr>
<tr>
<td></td>
<td>Blinking blue</td>
<td>Remote UID is on. Use this function through IPMI to identify the server from a remote location.</td>
</tr>
<tr>
<td>9b</td>
<td>Flashing</td>
<td>Indicates network activity on igb1 (upper left port).</td>
</tr>
<tr>
<td>9c</td>
<td>Flashing</td>
<td>Indicates network activity on igb0 (lower left port).</td>
</tr>
<tr>
<td>9d</td>
<td>Flashing</td>
<td>Indicates IDE channel activity on the hard drive.</td>
</tr>
<tr>
<td>9e</td>
<td>Illuminated</td>
<td>Indicates power is being supplied to the system power supply units. This LED should normally be illuminated when the system is operating.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Indicates no power is being supplied to the system power supply. System is powered off.</td>
</tr>
</tbody>
</table>
With CPIC-8955 Accelerator Card with Intel® QuickAssist Technology

<table>
<thead>
<tr>
<th>Port</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eno1</td>
<td>GigabitEthernet6/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>eno2</td>
<td>GigabitEthernet6/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>eno3</td>
<td>TenGigabitEthernet3/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>eno4</td>
<td>TenGigabitEthernet3/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

With 2 Port Intel 1 Gbps Ethernet Expansion Card

<table>
<thead>
<tr>
<th>Port</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ens2f0</td>
<td>GigabitEthernet5/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>ens2f1</td>
<td>GigabitEthernet5/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>eno1</td>
<td>GigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>eno2</td>
<td>GigabitEthernet7/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>eno3</td>
<td>TenGigabitEthernet3/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>6</td>
<td>eno4</td>
<td>TenGigabitEthernet3/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.
### With 2 Port Intel 10 Gbps X710 SFP+ Expansion Card

<table>
<thead>
<tr>
<th>Port</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TenGigabitEthernet5/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>TenGigabitEthernet5/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>GigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>GigabitEthernet7/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>TenGigabitEthernet3/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>6</td>
<td>TenGigabitEthernet3/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is `eno1`. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

### With 4 Port Intel 1 Gbps Ethernet Expansion Card

<table>
<thead>
<tr>
<th>Port</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ens2f0</td>
<td>GigabitEthernet5/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>ens2f1</td>
<td>GigabitEthernet5/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>ens2f2</td>
<td>GigabitEthernet5/0/2</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>ens2f3</td>
<td>GigabitEthernet5/0/3</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>eno1</td>
<td>GigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>6</td>
<td>eno2</td>
<td>GigabitEthernet7/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>7</td>
<td>eno3</td>
<td>TenGigabitEthernet3/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>8</td>
<td>eno4</td>
<td>TenGigabitEthernet3/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is `eno1`. The Host OS Interface is one network interface that is only available to
the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

With 4 Port Intel 10 Gbps X710 SFP+ Expansion Card

<table>
<thead>
<tr>
<th>Port</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TenGigabitEthernet5/0/3</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>TenGigabitEthernet5/0/2</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>TenGigabitEthernet5/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>TenGigabitEthernet5/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>GigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>6</td>
<td>GigabitEthernet7/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>7</td>
<td>TenGigabitEthernet3/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>8</td>
<td>TenGigabitEthernet3/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

Note: Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

Connecting to the Console Port

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

Additional Resources

Professional Services

Support does not cover more complex tasks such as network design and conversion from other firewalls. These items are offered as professional services and can be purchased and scheduled accordingly.

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

Netgate training offers training courses for increasing your knowledge of Netgate 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/

Resource Library

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

https://www.netgate.com/resources/

Warranty and Support

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

Enterprise Support is included with an active software subscription, for more information view the Netgate Global Support page.

See also:

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

1.1.5 Netgate 1541 Secure Router Manual

This Quick Start Guide covers the first time connection procedures for the Netgate 1541 1U Secure Router and also provides information needed to stay up and running.
Getting Started

Use the following steps to configure the TNSR Secure Router.

1. To configure the Network Interfaces and gaining access to the Internet, follow the instructions provided in the Zero-to-Ping documentation.

   **Note:** Not all steps in the Zero-to-Ping documentation will be necessary for every configuration scenario.

2. Once the Host OS is capable of reaching the Internet, check for updates (Updating TNSR) before proceeding. This ensures the security and integrity of the router before TNSR interfaces are exposed to the Internet.

3. Finally, configure the TNSR instance to meet the specific use case. The topics are listed on the left column of the TNSR Documentation site. There are also TNSR Configuration Example Recipes that might be of assistance when configuring TNSR.

Input and Output Ports

## Contents

- Input and Output Ports
  - Default Configuration
    - Network Ports
    - Other I/O
    - Status LEDs
  - With CPIC-8955 Accelerator Card with Intel® QuickAssist Technology
  - With 2 Port Intel 1 Gbps Ethernet Expansion Card
  - With 2 Port Intel 10 Gbps X710 SFP+ Expansion Card
  - With 4 Port Intel 1 Gbps Ethernet Expansion Card
  - With 4 Port Intel 10 Gbps X710 SFP+ Expansion Card

## Default Configuration

![Default Configuration Diagram]
Network Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eno1</td>
<td>GigabitEthernet6/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>eno2</td>
<td>GigabitEthernet6/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>eno3</td>
<td>TenGigabitEthernet3/0/0</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>eno4</td>
<td>TenGigabitEthernet3/0/1</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

Other I/O

<table>
<thead>
<tr>
<th>Port</th>
<th>I/O Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>IPMI</td>
</tr>
<tr>
<td>6</td>
<td>2x USB 3.0</td>
</tr>
<tr>
<td>7</td>
<td>VGA</td>
</tr>
<tr>
<td>8</td>
<td>Reset &amp; Power buttons</td>
</tr>
<tr>
<td>9</td>
<td>Status LEDs (see table below)</td>
</tr>
</tbody>
</table>

Status LEDs

![Status LEDs Image]

1.1. Netgate Appliances
<table>
<thead>
<tr>
<th>LED</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9a</td>
<td>Continuously on and red</td>
<td>An overheat condition has occurred. (This may be caused by cable congestion.)</td>
</tr>
<tr>
<td></td>
<td>Blinking red (1Hz)</td>
<td>Fan failure, check for an inoperative fan.</td>
</tr>
<tr>
<td></td>
<td>Blinking red (0.25Hz)</td>
<td>Power failure, check for a non-operational power supply.</td>
</tr>
<tr>
<td></td>
<td>Solid blue</td>
<td>Local UID has been activated. Use this function through IPMI to locate the server in a rack mount environment.</td>
</tr>
<tr>
<td></td>
<td>Blinking blue</td>
<td>Remote UID is on. Use this function through IPMI to identify the server from a remote location.</td>
</tr>
<tr>
<td>9b</td>
<td>Flashing</td>
<td>Indicates network activity on igb1 (upper left port).</td>
</tr>
<tr>
<td>9c</td>
<td>Flashing</td>
<td>Indicates network activity on igb0 (lower left port).</td>
</tr>
<tr>
<td>9d</td>
<td>Flashing</td>
<td>Indicates IDE channel activity on the hard drive.</td>
</tr>
<tr>
<td>9e</td>
<td>Illuminated</td>
<td>Indicates power is being supplied to the system power supply units. This LED should normally be illuminated when the system is operating.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Indicates no power is being supplied to the system power supply. System is powered off.</td>
</tr>
</tbody>
</table>
With CPIC-8955 Accelerator Card with Intel® QuickAssist Technology

<table>
<thead>
<tr>
<th>Port</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eno1</td>
<td>GigabitEthernet6/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>eno2</td>
<td>GigabitEthernet6/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>eno3</td>
<td>TenGigabitEthernet3/0/0</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>eno4</td>
<td>TenGigabitEthernet3/0/1</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

With 2 Port Intel 1 Gbps Ethernet Expansion Card

<table>
<thead>
<tr>
<th>Port</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ens2f0</td>
<td>GigabitEthernet5/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>ens2f1</td>
<td>GigabitEthernet5/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>eno1</td>
<td>GigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>eno2</td>
<td>GigabitEthernet7/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>eno3</td>
<td>TenGigabitEthernet3/0/0</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>6</td>
<td>eno4</td>
<td>TenGigabitEthernet3/0/1</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.
updating the host OS.

**With 2 Port Intel 10 Gbps X710 SFP+ Expansion Card**

<table>
<thead>
<tr>
<th>Port</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TenGigabitEthernet5/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>TenGigabitEthernet5/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>GigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>GigabitEthernet7/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>TenGigabitEthernet3/0/0</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>6</td>
<td>TenGigabitEthernet3/0/1</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

**With 4 Port Intel 1 Gbps Ethernet Expansion Card**
<table>
<thead>
<tr>
<th>Port</th>
<th>Linux Label</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ens2f0</td>
<td>GigabitEthernet5/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>ens2f1</td>
<td>GigabitEthernet5/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>ens2f2</td>
<td>GigabitEthernet5/0/2</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>ens2f3</td>
<td>GigabitEthernet5/0/3</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>eno1</td>
<td>GigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>6</td>
<td>eno2</td>
<td>GigabitEthernet7/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>7</td>
<td>eno3</td>
<td>TenGigabitEthernet3/0/0</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>8</td>
<td>eno4</td>
<td>TenGigabitEthernet3/0/1</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.

**With 4 Port Intel 10 Gbps X710 SFP+ Expansion Card**

<table>
<thead>
<tr>
<th>Port</th>
<th>TNSR Label</th>
<th>Port Type</th>
<th>Port Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TenGigabitEthernet5/0/3</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>2</td>
<td>TenGigabitEthernet5/0/2</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>3</td>
<td>TenGigabitEthernet5/0/1</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>4</td>
<td>TenGigabitEthernet5/0/0</td>
<td>SFP+</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>5</td>
<td>GigabitEthernet7/0/0</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>6</td>
<td>GigabitEthernet7/0/1</td>
<td>RJ-45</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>7</td>
<td>TenGigabitEthernet3/0/0</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>8</td>
<td>TenGigabitEthernet3/0/1</td>
<td>RJ-45</td>
<td>10 Gbps</td>
</tr>
</tbody>
</table>

**Note:** Default Host OS Interface is eno1. The Host OS Interface is one network interface that is only available to the host OS and not available in TNSR. Though technically optional, the best practice is to have one for accessing and updating the host OS.
Connecting to the Console Port

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

Additional Resources

Professional Services

Support does not cover more complex tasks such as network design and conversion from other firewalls. These items are offered as professional services and can be purchased and scheduled accordingly.

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

Netgate Training

Netgate training offers training courses for increasing your knowledge of Netgate 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/

Resource Library

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

https://www.netgate.com/resources/

Warranty and Support

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

Enterprise Support is included with an active software subscription, for more information view the Netgate Global Support page.

See also:

For more information on how to use TNSR® software, see the TNSR Documentation and Resource Library.
1.2 Cloud Platforms

TNSR Secure Networking software is available in the following Cloud Platforms.

- **Amazon Web Services** - Instances with Enhanced Network Adapters (ENA)
- **Microsoft Azure** - Instances with Accelerated Networking

1.2.1 TNSR for Amazon AWS

The Netgate® TNSR Router for Amazon AWS is a powerful routing and VPN appliance. TNSR leverages vector packet processing and acceleration techniques for extremely high speed routing and VPN performance. A TNSR instance running in AWS can securely connect between AWS and remote offices, data centers, or even make high speed links between AWS regions.

TNSR for AWS is available in the AWS Marketplace.

**Note:** Visit the TNSR product page for additional information on purchasing access to TNSR on AWS.

Getting Started

Prerequisites and Requirements

Using a Netgate® appliance instance to protect VPC subnets requires the following:

- Setup can take 30 minutes to two hours, depending on the user’s familiarity with the tools.
- An AWS Account.
- Familiarity with AWS networking.
- A VPC.
- One internet-facing subnet, to which the Netgate appliance instance will have its internet-facing WAN interface connected.
- Two or more private subnets, to which the Netgate appliance instance will have its host management interface, client-facing LAN interface, and possibly additional optional interfaces connected.
- Separate routing tables for the internet-facing subnet and the private subnets.
- Separate security groups for the internet-facing subnet and the private subnets.
- An elastic IP address or public IP address for the WAN interface of the appliance.

For the purposes of this guide, the VPC will contain three subnets (one public and two private) as well as an Internet Gateway. The end result should look like the following diagram:

If all of these are already in place with an existing VPC, feel free to skip ahead to Launching an Instance.
Fig. 17: Architecture Diagram
Choosing Instance Type and Sizing

There are a range of specifications to choose from and this page will help guide through those choices.

Supported EC2 Instance Types

An instance type will depend on the expected network throughput as well as the types of services the Netgate® appliance will provide.

The available instance types are those that support ENA network adapters. These include all C5 and M5 instance types. The type of C5 or M5 instance depends on the needs of a given network. For networks with a large number of subnets in the VPC or for networks that expect high throughput, one of the larger instance types is likely to be more appropriate.

For information on bandwidth limits and limits on the number of Network Interfaces and IP addresses for different instance types, see the following links:

- https://aws.amazon.com/ec2/instance-types/

In environments where the requirements are unclear, start with c5.xlarge and migrate to a different instance type later as necessary.

Sizing the Storage

For general purpose routers, storage requirements will typically be small and the default 10GB volume should be sufficient.

In situations where the appliance may be customized with additional local software, or other advanced features outside of TNSR, consider increasing the volume size to something more appropriate, for example 64GB.

AWS Service Limits

New services provisioned in a VPC may be assigned IP addresses or other resources, but Amazon puts limits on VPC resources per Region. Before provisioning a new resource, make sure to check these limits.

The following tables list the limits for Amazon VPC resources per Region. Unless indicated otherwise, requests can be made to increase these limits using the Amazon VPC limits form. For some of these limits, the current limit applied can be viewed using the Limits page of the Amazon EC2 console.

**Note:** If a limit increase is requested that applies per resource, AWS increases the limit for all resources in the Region. For example, the limit for security groups per VPC applies to all VPCs in the Region.
VPC and Subnets

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPCs per Region</td>
<td>5</td>
<td>The limit for Internet gateways per Region is directly correlated to this one. Increasing this limit increases the limit on internet gateways per Region by the same amount.</td>
</tr>
<tr>
<td>Subnets per VPC</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>IPv4 CIDR blocks per VPC</td>
<td>5</td>
<td>This limit is made up of the primary CIDR block plus 4 secondary CIDR blocks.</td>
</tr>
<tr>
<td>IPv6 CIDR blocks per VPC</td>
<td>1</td>
<td>This limit cannot be increased.</td>
</tr>
</tbody>
</table>

DNS

For more information, see DNS Limits.
Elastic IP Addresses (IPv4)

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elastic IP addresses per Region</td>
<td>5</td>
<td>This is the limit for the number of Elastic IP addresses for use in EC2-VPC. For Elastic IP addresses for use in EC2-Classic, see Amazon EC2 Limits in the Amazon Web Services General Reference.</td>
</tr>
</tbody>
</table>

Flow Logs

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow logs per single network interface, single subnet, or single VPC in a Region</td>
<td>2</td>
<td>This limit cannot be increased. There can effectively be 6 flow logs per network interface by creating 2 flow logs for the subnet, and 2 flow logs for the VPC in which the network interface resides.</td>
</tr>
</tbody>
</table>
# Gateways

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer gateways per Region</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Egress-only internet gateways per Region</td>
<td>5</td>
<td>This limit is directly correlated with the limit on VPCs per Region. To increase this limit, increase the limit on VPCs per Region. Only one egress-only internet gateway can attach to a VPC at a time.</td>
</tr>
<tr>
<td>Internet gateways per Region</td>
<td>5</td>
<td>This limit is directly correlated with the limit on VPCs per Region. To increase this limit, increase the limit on VPCs per Region. Only one internet gateway can be attached to a VPC at a time.</td>
</tr>
<tr>
<td>NAT gateways per Availability Zone</td>
<td>5</td>
<td>A NAT gateway in the pending, active, or deleting state counts against the limit.</td>
</tr>
</tbody>
</table>
Creating an IAM User in an AWS Account

A TNSR® AMI uses AWS Identity and Access Management (IAM) accounts for administration. Every AWS account includes at least one user. For security reasons, the root account should not be used for day-to-day administration. This section describes the process of creating and using an IAM user account for administrating the TNSR® AMI.

See also:

To find out more about AWS security and credentials read Understanding and Getting Your Security Credentials.

There are multiple methods for creating users in IAM. The recommended method is to use the AWS Management Console. The process of creating a user and enabling that user to perform work tasks consists of the following steps:

1. Create the user.
2. Create credentials for the user.
3. As a best practice, create only the credentials that the user needs. For example, for a user who requires access only through the AWS Management Console, do not create access keys.

Note: For cloud security the best practice is to limit access for the root account, so the root account is locked by default.

4. Grant the appropriate permissions to the user to administer the TNSR® AMI.
5. Provide the user with the necessary sign-in information.
6. (Optional) Configure multi-factor authentication (MFA) for the user.

Creating IAM Users (Console)

The AWS Management Console can create IAM users.

To create one or more IAM users (console):

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Users and then choose Add user.
3. Type the user name for the new user. This is the name they will use to sign in to AWS. To add up to 10 users at once, choose Add another user for each additional user and type their user names.
4. User names can be a combination of up to 64 letters, digits, and these characters: +=,.@-
5. Names must be unique within an account and are not case sensitive.
6. Select AWS Management Console access. This creates a password for each new user.

Choose one of the following options for Console password:

- **Autogenerated password**
  Each user gets a randomly generated password that meets the account password policy in effect (if any).

  **Note:** The Final page allows viewing or downloading the passwords.

- **Custom password**
  Each user is assigned a given password.
Tip: The best practice is to select Require password reset to ensure that users are forced to change their password the first time they sign in.

7. Click Next. On the Set permissions page, specify how to assign permissions to this new user(s). Choose one of the following three options:

   Add user to group
   Choose this option to assign the user(s) to one or more groups that already have permissions policies. IAM displays a list of the groups in the account, along with their attached policies.
   Select one or more existing groups or choose Create group to create a new group.

   Copy permissions from existing user
   Choose this option to copy all access rights from an existing user to the new user(s).

   Attach existing policies to user directly
   Choose this option to see a list of the managed policies in the account. Select the policies to attach to the new users or choose Create policy to open a new browser tab and create a new policy.

8. Choose Next: Review to see all of the choices made up to this point. Choose Create user to proceed.

9. To view user access keys (access key IDs and secret access keys), choose Show next to each password and access key to display. To save the access keys, choose Download .csv and then save the file to a secure location.

   Danger: This is the only opportunity to view or download the secret access keys, and users must have this information before they can use the AWS API. Save the user new access key ID and secret access key in a safe and secure place.
   There is no way to access the secret keys again after this step.

10. Choose Send email next to each user to send a message with account information. This opens a local mail client with a draft that to customize and send. The email template includes the following details to each user:

   • User name
   • URL to the account sign-in page. Use the following example, substituting the correct account ID number or account alias:
   • https://AWS-account-ID or alias.signin.aws.amazon.com/console

   Important: The user’s password is not included in the generated email as email is not a secure communications channel. Provide passwords to the user in a secure way that complies with security policies set by the organization.

Using IAM Roles

AWS IAM Roles are used to delegate access to users, applications, or services that require controlled access to AWS resources. IAM Roles should be used to manage all Netgate® TNSR® software instances. This unique role can be specified when launching a new instance, or attached to an existing instance.

The AWS Management Console is the recommended method for creating roles for use with TNSR® software. The best practice is to create these roles based on the principle of least privilege, also known as the principle of least authority, which is the assignment of lowest needed privileges based on necessity. These instructions attempt to follow this principle.
Create Policy for TNSR Software Management IAM Role

Create a custom policy that will be associated with an IAM role allowing access to the TNSR® Management GUI running on an EC2 Instance.

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the console, select Policies then choose Create Policy.
3. Drop down the Service menu and select EC2.
4. In the Actions dropdown check the box next to All EC2 actions (ec2:)

Note: If stricter policies are required for the actions that can be performed on the TNSR® EC2 Instance, these can be set here.

5. Select the Resources dropdown arrow and review resulting warnings.
6. Click the All resources bubble
7. Select Review policy.
8. Populate the Name field (e.g. TNSR_EC2_Access) and Description, if desired.

Note: Policy names must be unique within the AWS account, and the name of the policy cannot be changed once created.

9. Select Create Policy.

Create IAM Role for TNSR Software Management

Create a role that an IAM user, or users within an IAM Group, can assume and use to connect to and manage TNSR® running on an EC2 Instance.

Note: The administrator of the specified account can grant permission to assume this role to any IAM user in that account. To do this, the administrator attaches a policy to the user or a group that grants permission for the sts:AssumeRole action. That policy must specify the role’s ARN as the Resource.

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the console, select Roles then choose Create Role.
3. Select the Another AWS account role type.
4. In the Account ID field, type the AWS account ID that will be allowed to access the destination resource.
5. The Require external ID checkbox should remain cleared unless granting permissions to users from an account not under the control of this organization. Reference AWS Documentation for External ID Roles in the event this is required.
6. The best practice is to restrict the role to users who sign in with multi-factor authentication (MFA). Select Require MFA to add a condition to the role’s trust policy to require MFA sign-in.
7. Select Next: Permissions.
8. Type the name of the previously created Custom policy in the search field. Check the box next to the correct Policy name.

9. Select Next: Tags

   **Note:** IAM tags are key-value pairs that can be used to organize, track, or control access for this role. This is an optional step. More information can be found within AWS Documentation for Tagging IAM Entities.

10. Select Next: Review.

11. Populate the **Role name** field (e.g. **TNSR_Admin**) and Role description if desired.

   **Note:** Role names must be unique within the AWS account, and the name of the role cannot be changed once created.

12. Review remaining configured settings then select **Create role**.

This role can now be assigned to an IAM User or all users in an IAM group allowing secure administrative access to the EC2 Instance(s) containing TNSR®.

### Instance Usage

#### Launching an Instance

These instructions cover how to launch a new instance of the Netgate® TNSR® appliance from the Amazon EC2 Management Console.

1. Login to AWS, for example by navigating to [https://console.aws.amazon.com/](https://console.aws.amazon.com/)

   **Note:** This URL may be different if using other login functions, such as an IAM role or SSO authentication.

2. Select the region for the instance to run in:
   - Click the current **Region** name near the upper right corner of the page
   - Select a new region if necessary
3. Navigate to the EC2 console

- Click Services near the top left corner of the page
- Click Compute on the left navigation menu
- Click EC2 on the main section of the menu

4. Enter the Launch Instance Wizard

- Click the Launch Instance button to open the Launch Instance menu

This button is in the Launch Instance section which is located under the Resources section of the EC2
• Click **Launch Instance** from the menu

5. Give the new instance a **Name**, such as TNSR

   Optionally, click **Add Additional Tags** to create more tags which can be used to identify and locate this instance.

6. Type **Netgate TNSR** in the search box and press **Enter**.
7. Select **AWS Marketplace AMIs** if it is not automatically highlighted

8. Click the **Select** button for the **Netgate TNSR vRouter** entry in the search results.
9. Review pricing and other helpful information, then click **Continue**.

**Note:** TNSR software is also available with an annual subscription instead of hourly. The annual subscription may be purchased from the AWS Marketplace. Information about support can be found on the **Support Resources** page.

10. Choose an **Instance Type** from the drop-down, then click **Next**

**See also:**

For guidance on which instance type to choose, see **Supported EC2 Instance Types**.

11. Configure an **SSH Key Pair**

The **Key Pair** section of the form sets the SSH key pair used by an SSH client when it connects to the TNSR instance for management.

For an existing key pair:

- Click **Key pair name**
• Search for and select an existing key pair entry

To create a new key pair:

• Click **Create new Key Pair**
• Enter a **Key pair name**, such as **TNSR SSH Key**
• Select a **Key Pair Type** and **Private Key Format**
  The chosen type and format must be compatible with whichever local SSH client will be used by TNSR administrators
• Click the **Create key pair**
• Select a location to save the key pair locally

---

**Create key pair**

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

**Key pair name**

**My SSH Key**

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

**Key pair type**

- **RSA**
  RSA encrypted private and public key pair
- **ED25519**
  ED25519 encrypted private and public key pair (Not supported for Windows instances)

**Private key file format**

- **.pem**
  For use with OpenSSH
- **.ppk**
  For use with PuTTY

---

12. Click **Edit** under **Network Settings** to allow making changes for the next few steps.
13. Configure Security Groups

The default security group only includes a rule to allow SSH. Since this group is for the management interface, allowing additional traffic is unlikely to be necessary, but there are still a few changes to make:

- Click Create security group under Firewall (security groups)
- Enter a Security group name, such as TNSR Management or leave it at the default automatic value.
- Enter a Description for the group, or leave it at the default value.
- Set the Source type on the default rule for SSH to My IP so it will restrict SSH access to the public address used by the person creating the AMI.

This is optional, but more secure. If the address is not static, then it may not be viable to restrict this. Setting the value to Anywhere will allow SSH clients to connect from any source (0.0.0.0/0). While not ideal, allowing SSH connection from anywhere is OK because the TNSR for AWS default setup only allows key-based SSH authentication which is resistant to brute force attacks.

14. Configure Network and Interfaces

- Select the VPC in which to launch the instance
- Click Advanced Network Configuration to expand the network interface list
- Select the Management subnet as the subnet for Network Interface 1
• Click the **Add Network Interface** button
• Select the **WAN subnet** as the subnet for **Network Interface 2**
• Click the **Add Network Interface** button
• Select the **LAN subnet** as the subnet for **Network Interface 3**

15. **Configure storage**

   If this instance will require more than the default 8 GiB disk, increase the value in the **Configure Storage** section

16. Verify the settings selected in earlier steps and review any errors or recommendations displayed by AWS

17. Click **Launch instance** in the **Summary** box on the right side

---

**1.2. Cloud Platforms**
Managing the Configuration of the Instance

Once the instance is launched, monitor its status using the **Instances** page of the EC2 Management Console. The EC2 Management Console will display a list of instances. In this list it also indicates whether an instance is up and reachable and will also display its current public IP address and other related basic information.

Click the checkbox at the start of the row for an instance to display more information.
With the instance selected, the bottom pane of the page displays detailed information about the instance. This includes the hostname and all IP address on the instance.

To manage the configuration of the instance, connect to it via SSH as described in Connect to the instance.

**Advanced Usage**

**Protecting a private network in VPC**

An instance of the Netgate® TNSR® appliance can be used as a firewall for a VPC subnet. This will generally require more manual configuration than using an instance to host a remote access VPN does. See the VPC User Guide for a more detailed explanation of how to configure a VPC and a Netgate TNSR® appliance instance to support this.
Connecting local devices using IPsec

A TNSR instance in AWS can act as an IPsec hub for one or more remote endpoints capable of using IPsec, such as local devices running pfSense® software. It can interconnect all of the sites or even act as an Internet gateway.

For a complete example of using TNSR as an IPsec hub for multiple sites running pfSense software, see the recipe TNSR IPsec Hub for pfSense software nodes in the TNSR documentation.

Accessing the TNSR API

Accessing the API requires configuring the RESTCONF service in a secure manner as well as setting up a means of user authentication and NACM rules for authorization. There is a complete recipe in the TNSR documentation: RESTCONF Service Setup with Certificate-Based Authentication and NACM

Warning: Ideally, the API should only be accessed from the management interface or at least over an encrypted channel such as a VPN.

For more information on the API in general, see the API Documentation.

Detect and Recover EC2 Instance Failure

It is also possible to create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying issue.

For more information about instance recovery, see Recover Your Instance.

Frequently Asked Questions

How can an instance be accessed?

In order to manage the configuration of the instance, connect to it via SSH as described in Connect to the instance.

What are the default credentials for the tnsr user on the AWS instance?

The tnsr user on the TNSR for AWS instance does not have a default password. SSH connections to a TNSR for AWS instance require key-based authentication using an SSH key selected when launching the instance, which is much more secure than using password-based authentication.

The process of using key-based authentication to connect to an instance is covered in Connect to the instance.
How does NAT behave on AWS?

NAT behavior on AWS can be tricky, as in certain places NAT can be applied by TNSR and in other places by AWS. Determining where and how to perform NAT can be potentially problematic in that it is possible to unintentionally create asymmetric routing situations with an incorrect configuration.

See NAT Examples for multiple examples of NAT behavior with TNSR on AWS and how to avoid these pitfalls.

How can an instance be backed up and recovered?

The procedure to backup and restore the configuration databases and other key files is covered in the Configuration Backups section of the TNSR documentation.

How can an instance be monitored?

TNSR can be monitored in several ways compatible with standard utilities, such as SNMP, IPFIX, and Prometheus as well as customized monitoring by polling the TNSR API. The most common methods are covered in the Monitoring section of the TNSR documentation.

How can an instance be upgraded?

Upgrading a TNSR instance in-place requires a valid upgrade certificate issued by Netgate. The process for obtaining the certificate as well as for performing the upgrade is covered in the Updates and Packages section of the TNSR documentation.

Note: Requesting a TNSR upgrade certificate from Netgate TAC requires the current AWS Customer ID and AWS Instance ID. For more details, see the documentation on upgrading TNSR in AWS

Even without the TNSR upgrade configuration in place, the operating system can be upgraded to obtain security fixes for issues in the base OS.

How can credentials and keys be changed?

Credentials and keys, such as user account keys, certificates, VPN tunnel keys, and so on, should be changed periodically for security. Procedures to change these are located in Changing Credentials and Keys.

Further troubleshooting

More information on troubleshooting a variety of common TNSR issues can be found in the Troubleshooting section of the TNSR documentation.
Virtual Private Cloud (VPC)

AWS TNSR Instance Setup

This zero-to-ping setup guide will explain how to get started using TNSR to route network traffic in an AWS VPC environment.

The steps involved are:

Learn the Basics

TNSR utilizes an optimized userspace data plane to forward packets at very high rates. On AWS, TNSR runs on a customized VM instance and is managed by connecting to a command-line interface (CLI) over SSH.

There are many different network designs possible in AWS. This guide assumes a TNSR instance will sit in a VPC connected to a private subnet and a public subnet (one which has access to the Internet).

This guide will show how to bring up a TNSR instance with 3 Elastic Network Adapter interfaces attached:

Management Interface

The primary network interface on the instance is used for management of the TNSR instance. This is the interface reached via SSH to connect to the CLI on the TNSR instance. Packets received on this interface will not be forwarded to another interface. The interface is used for system functions such as DNS resolution and downloading software updates.

The management interface is required.

TNSR WAN/Internet Interface

The TNSR WAN interface is used by TNSR to connect to the Internet. A WAN interface will have an Elastic IP Address assigned and it will be attached to a subnet that has a route to an Internet Gateway in its Route Table.

TNSR LAN/Private Interface

The TNSR LAN interface connects TNSR to a private Subnet in the VPC. The instances in the private subnet do not have their own Elastic IP Addresses and the Route Table for the subnet does not have a route to an Internet Gateway, but instead has a route to the TNSR LAN interface.

Instances on the private subnet will use TNSR as their gateway to the Internet.

Each of the three network interfaces resides on a distinct subnet.

The examples in this guide use the following configuration:

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC Address Space</td>
<td>10.5.0.0/16</td>
</tr>
<tr>
<td>WAN Subnet</td>
<td>10.5.0.0/24</td>
</tr>
<tr>
<td>LAN Subnet</td>
<td>10.5.1.0/24</td>
</tr>
<tr>
<td>Management Subnet</td>
<td>10.5.2.0/24</td>
</tr>
</tbody>
</table>

In a real production VPC, the TNSR instance may have more than one WAN interface and/or more than one LAN interface. The concepts covered in this guide can be extended to additional interfaces.
Launch an Instance

To launch this instance, follow the procedure in Launching an Instance.

Add TNSR LAN Interface to the Instance

The Management and WAN Interfaces were created while launching the instance. Now create the LAN interface. If this instance requires additional interfaces, either public or private, create those now.

To allocate a new TNSR LAN Network Interface, create a new Elastic Network Interface on the LAN subnet following the instructions here https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#create_eni

The subnet connected to the TNSR LAN interface is a private network which is using the TNSR instance as its Internet gateway. It can have a much less restrictive Security Group set so that traffic from the LAN can reach the TNSR instance. Select the default Security Group for the VPC, which should allow all inbound traffic.

Note: The Description field is optional when creating a Network Interface but the best practice is to enter Description text that identifies the interface so it can be easily identified when it is attached to an instance.

To attach the LAN Network Interface to the instance, follow the instructions at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#attach_eni_running_stopped

Prepare TNSR Network Interfaces

The TNSR WAN and LAN interfaces should have Source/Destination Check disabled in order to allow the TNSR instance to route packets. If these settings are not disabled, packets from the LAN subnet to the Internet will be dropped before reaching the TNSR LAN interface.

To disable Source/Destination Check for a Network Interface, follow the instructions at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#change_source_dest_check

Connect Management and WAN Interfaces to the Internet

The Management Interface and the TNSR WAN interface must be assigned public Elastic IP Addresses by AWS.

For each interface that needs a public Elastic IP Address, allocate one by following the instructions at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html#using-instance-addressing-eips-allocating

Make a note of the allocated Elastic IP Address.

Before associating an Elastic IP Address to a Network Interface, make a note of the ID of the Network Interface to use. To find the Network Interface ID:

1. Navigate to https://console.aws.amazon.com/ec2/
2. Click Instances
3. Click the button next to the TNSR interface to select it
4. Look at the bottom of the page, under the Description tab to see Network Interfaces
5. Click on the interface names to display information about the Network Interface:
   - eth0 for management interface
   - eth1 for WAN interface
6. Write down the **Interface ID** for each interface

After allocating the Elastic IP Addresses and finding the Network Interface IDs for eth0 and eth1, associate the Elastic IP Addresses to the Network Interfaces by following the instructions at [https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#associate_eip](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#associate_eip)

**Connect to the instance**

The TNSR instance does not have a default password. SSH connections to this instance require key-based authentication using an SSH key selected when launching the instance.

The default account is named *tnsr*.

**Note:** The *root* account is present on the appliance but disabled by default. It is not necessary to enable or use the *root* account. Any administrative actions can be taken using the *tnsr* account from within the TNSR CLI or by using *sudo* from a shell prompt.

See [Default Accounts and Passwords](#) for additional information.

To connect from a shell prompt in a Unix/Linux terminal:

```
$ ssh -i <my_key_file> tnsr@<eth0_public_ip_addr>
```

Substitute the actual key file name instead of typing *<my_key_file>* and the management interface Elastic IP Address instead of typing *<eth0_public_ip_addr>*.

The ssh client will print a warning similar to:

```
The authenticity of host 'x.x.x.x' can't be established.
ECDSA key fingerprint is SHA256:6/LDXVPpD2v6hnWdFHFWhkCsbMcah4tBgtuDLAa40.
Are you sure you want to continue connecting (yes/no)?
```

This warning only appears the first time connecting using SSH on a given system and user account. Type yes to continue connecting.

If all went well, the TNSR CLI will automatically be launched, resulting in output similar to the following:

```
Netgate TNSR
Version: v0.1.0-567-g0967ac3
Build timestamp: Fri Apr 20 16:16:48 2018 CDT
Git Commit: 0x967ac3d
ip-10-5-2-225.ec2.internal tnsr#
```

**Tip:** Additional host users can be added to TNSR so that each administrator can use their own account. See the [User Management](#) section of the TNSR documentation for details.
Configure Interface Addresses in TNSR

Now that the TNSR CLI is open, start configuring the TNSR instance. First, configure the network interfaces and bring them up.

Since the TNSR LAN interface was added to the instance after launching the instance, it will not be visible yet to the TNSR data plane unless the instance has been rebooted. Check which interfaces are visible to TNSR by typing `show interface` at the CLI prompt.

Here’s an example of what will appear:

```
  tnsr# show interface
  Interface: VirtualFunctionEthernet0/6/0
    Admin status: down
    Link down, 100 Gbit/sec, full duplex
    Link MTU: 9216 bytes
    MAC address: 0a:54:d0:7c:df:c0
    IPv4 Route Table: ipv4-VRF:0
    IPv6 Route Table: ipv6-VRF:0
    counters:
      received: 0 bytes, 0 packets, 0 errors
      transmitted: 0 bytes, 0 packets, 0 errors
      0 drops, 0 punts, 2 rx miss, 0 rx no buffer
```

Only one interface is visible on this instance: the WAN interface which was attached at the time the instance launched.

If all of the TNSR instances, other than the Management Interface, are not displayed by `show interface`, restart the data plane and the missing interfaces will appear:

```
  tnsr# configure
  tnsr(config)# service dataplane restart
  Success
  tnsr(config)# exit
```

Check the interfaces again:

```
  tnsr# show interface
  Interface: VirtualFunctionEthernet0/6/0
    Admin status: down
    Link down, 100 Gbit/sec, full duplex
    Link MTU: 9216 bytes
    MAC address: 0a:54:d0:7c:df:c0
    IPv4 Route Table: ipv4-VRF:0
    IPv6 Route Table: ipv6-VRF:0
    counters:
      received: 0 bytes, 0 packets, 0 errors
      transmitted: 0 bytes, 0 packets, 0 errors
      0 drops, 0 punts, 2 rx miss, 0 rx no buffer

  Interface: VirtualFunctionEthernet0/7/0
    Admin status: down
    Link down, 100 Gbit/sec, full duplex
    Link MTU: 9216 bytes
    MAC address: 0a:0a:7b:cd:89:6e
    IPv4 Route Table: ipv4-VRF:0
```

(continues on next page)
IPv6 Route Table: ipv6-VRF:0
counters:
  received: 0 bytes, 0 packets, 0 errors
  transmitted: 0 bytes, 0 packets, 0 errors
  0 drops, 0 punts, 0 rx miss, 0 rx no buffer

After the restart a second interface is visible: the TNSR LAN interface.

When all of the interfaces that are attached are present, the instance is ready to start enabling and configuring IP addresses on interfaces.

During the process of creating Network Interfaces, a private IP address was assigned to each interface. The next step is to configure those addresses on the interfaces in TNSR in order to communicate with other instances in the VPC.

Configure WAN interface:

1. Navigate to https://console.aws.amazon.com/ec2/
2. Click Instances
3. Click the button next to the TNSR interface to select it
4. Look at the bottom of the page, under the Description tab to see Network Interfaces
5. Click on eth1
6. Find the field named “Private IP address” in the popup
7. Configure the interface in the CLI:

```
tnsr# configure
tnsr(config)# interface VirtualFunctionEthernet0/6/0
tnsr(config-interface)# ip address 10.5.0.222/24
tnsr(config-interface)# enable
tnsr(config-interface)# description eth1 eni-beaa7c21 WAN
tnsr(config-interface)# exit
```

This sets an address, brings up the interface, and sets a description to serve as a reminder of the interface identity & purpose.

Substitute a different Private IP address/mask and description as needed.

Configure LAN interface:

1. Navigate to https://console.aws.amazon.com/ec2/
2. Click Instances
3. Click the button next to the TNSR interface to select it
4. Look at the bottom of the page, under the Description tab to see Network Interfaces
5. Click on eth2
6. Find the field named “Private IP address” in the popup
7. Configure the interface in the CLI:

```
tnsr(config)# interface VirtualFunctionEthernet0/7/0
tnsr(config-interface)# ip address 10.5.1.218/24
tnsr(config-interface)# enable
tnsr(config-interface)# description eth2 eni-6fa572f0 LAN
```

(continues on next page)
Again, substitute the interface Private IP address/mask and description as needed.

Check interface status again:

```
tnsr# show interface
Interface: VirtualFunctionEthernet0/6/0
  Description: eth1 eni-beaa7c21 WAN
  Admin status: up
  Link up, unknown, unknown duplex
  Link MTU: 9216 bytes
  MAC address: 0a:54:d0:7c:df:c0
  IPv4 Route Table: ipv4-VRF:0
  IPv4 addresses:
  10.5.0.222/24
  IPv6 Route Table: ipv6-VRF:0
  counters:
    received: 798 bytes, 19 packets, 0 errors
    transmitted: 1604 bytes, 28 packets, 0 errors
    0 drops, 0 punts, 5 rx miss, 0 rx no buffer

Interface: VirtualFunctionEthernet0/7/0
  Description: eth2 eni-6fa572f0 LAN
  Admin status: up
  Link up, unknown, unknown duplex
  Link MTU: 9216 bytes
  MAC address: 0a:0a:7b:cd:89:6e
  IPv4 Route Table: ipv4-VRF:0
  IPv4 addresses:
  10.5.1.218/24
  IPv6 Route Table: ipv6-VRF:0
  counters:
    received: 1925 bytes, 30 packets, 0 errors
    transmitted: 1226 bytes, 19 packets, 0 errors
    20 drops, 0 punts, 27 rx miss, 0 rx no buffer
```

The output shows that the interfaces are up and configured, and the counters show that a few packets have been received.

It is now possible to verify connectivity to the VPC gateway on each subnet with the `ping` command. The VPC gateway address is the base address of a subnet + 1. e.g.:

- VPC gateway IP address for 10.5.0.0/24:
  
  Base address 10.5.0.0 + 1 = 10.5.0.1

- VPC gateway IP address for 10.5.1.0/24: 10.5.1.1

  Base address 10.5.1.0 + 1 = 10.5.1.1

```
tnsr# ping 10.5.0.1 source 10.5.0.222 count 3
PING 10.5.0.1 (10.5.0.1) 56(84) bytes of data.
64 bytes from 10.5.0.1: icmp_seq=1 ttl=64 time=0.096 ms
64 bytes from 10.5.0.1: icmp_seq=2 ttl=64 time=0.231 ms
```
Interface Naming

The names that are displayed for Network Interfaces on an instance in the EC2 Web Console are different than the names that appear in the TNSR CLI. The interfaces in TNSR are named using the PCI bus/slot/function of the device. The names in the EC2 Web Console use the traditional Linux naming scheme and display as `eth0`, `eth1`, and so on.

In this example, it is straightforward to determine which interface in TNSR corresponds to an AWS Network Interface in the EC2 Web Console because there are only 2 interfaces and one of them will be present at boot time.

If this instance has more Network Interfaces than in the example, or if it is unclear which interface in the TNSR CLI matches up with which Network Interface in the EC2 Web Console, the two can be correlated by checking the MAC addresses. The TNSR CLI command `show interface` will display all of the interfaces present and the output includes the MAC address of each. The MAC address of each TNSR interface can be checked in the EC2 Web Console to find the right Network Interface.

To find the MAC address of a Network Interface in the EC2 Web Console:

1. Navigate to https://console.aws.amazon.com/ec2/
2. Click Instances
3. Click the button next to the TNSR interface to select it
4. Look at the bottom of the page, under the Description tab to see Network Interfaces
5. The eth0 interface it the management interface and won’t appear in the TNSR CLI. Look at eth1, eth2, etc.
6. Click on the interface name to display information about the Network Interface
7. Click on the Interface ID to open the Network Interfaces page
   
   Only the Network Interface matching the selected ID will be displayed.
8. Look at the bottom of the page, under the Details tab, to find the “MAC address” field.
9. Match this MAC address to one of the MAC addresses printed from the show interface output in the CLI
Configure Default Route in TNSR

In order for the TNSR data plane to forward packets outside of the VPC to the Internet, a default route needs to be configured which sets a next hop of the VPC gateway for the WAN subnet using the TNSR CLI.

Configure a default route:

```
tnsr# configure
tnsr(config)# route ipv4 table ipv4-VRF:0
tnsr(config-route-table-v4)# route 0.0.0.0/0
tnsr(config-rttbl4-next-hop)# next-hop 1 via 10.5.0.1 VirtualFunctionEthernet0/6/0
tnsr(config-rttbl4-next-hop)# exit
tnsr(config-route-table-v4)# exit
tnsr(config)# exit
tnsr#
```

Ping TNSR WAN Interface from local network

The instance should now be reachable via ICMP echo request (ping) using the Elastic IP Address associated to the TNSR WAN Interface.

To find the Elastic IP address associated to the TNSR WAN Interface, use the EC2 Web Console:

1. Navigate to https://console.aws.amazon.com/ec2/
2. Click Instances
3. Click the button next to the TNSR interface to select it
4. Look at the bottom of the page, under the Description tab to see Network Interfaces
5. Click on eth1
6. Find the Elastic IP Address field in the popup

Now, try to ping the Elastic IP Address of the TNSR WAN Interface:

```
bash-3.2$ ping -c 5 52.7.26.219
PING 52.7.26.219 (52.7.26.219): 56 data bytes
64 bytes from 52.7.26.219: icmp_seq=0 ttl=45 time=48.781 ms
64 bytes from 52.7.26.219: icmp_seq=1 ttl=45 time=49.232 ms
64 bytes from 52.7.26.219: icmp_seq=2 ttl=45 time=49.238 ms
64 bytes from 52.7.26.219: icmp_seq=3 ttl=45 time=48.632 ms
64 bytes from 52.7.26.219: icmp_seq=4 ttl=45 time=48.433 ms
--- 52.7.26.219 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 48.433/48.863/49.238/0.323 ms
```

**Warning:** Once the Host OS is capable of reaching the Internet, check for updates (Updating TNSR) before proceeding. This ensures the security and integrity of the router before TNSR interfaces are exposed to the Internet.
References

Regional Market Availability

The tables below represent the current availability by regional market. If the desired regional market is not listed, refer to the AWS Regions availability or submit a support ticket directly to AWS.

Table 5: AWS Available Regions

<table>
<thead>
<tr>
<th>Market</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-east-1 N. Virginia</td>
<td>Available</td>
</tr>
<tr>
<td>us-east-2 Ohio</td>
<td>Available</td>
</tr>
<tr>
<td>us-gov-east-1 GovCloud East</td>
<td>Available</td>
</tr>
<tr>
<td>us-gov-west-1 GovCloud West</td>
<td>Available</td>
</tr>
<tr>
<td>us-west-1 N. California</td>
<td>Available</td>
</tr>
<tr>
<td>us-west-2 Oregon</td>
<td>Available</td>
</tr>
<tr>
<td>af-south-1 Cape Town</td>
<td>Available</td>
</tr>
<tr>
<td>ap-east-1 Hong Kong</td>
<td>Available</td>
</tr>
<tr>
<td>ap-northeast-1 Tokyo</td>
<td>Available</td>
</tr>
<tr>
<td>ap-northeast-2 Seoul</td>
<td>Available</td>
</tr>
<tr>
<td>ap-south-1 Mumbai</td>
<td>Available</td>
</tr>
<tr>
<td>ap-southeast-1 Singapore</td>
<td>Available</td>
</tr>
<tr>
<td>ap-southeast-2 Sydney</td>
<td>Available</td>
</tr>
<tr>
<td>ca-central-1 Quebec</td>
<td>Available</td>
</tr>
<tr>
<td>eu-central-1 Frankfurt</td>
<td>Available</td>
</tr>
<tr>
<td>eu-north-1 Stockholm</td>
<td>Available</td>
</tr>
<tr>
<td>eu-south-1 Milan</td>
<td>Available</td>
</tr>
<tr>
<td>eu-west-1 Ireland</td>
<td>Available</td>
</tr>
<tr>
<td>eu-west-2 London</td>
<td>Available</td>
</tr>
<tr>
<td>eu-west-3 Paris</td>
<td>Available</td>
</tr>
<tr>
<td>sa-east-1 São Paulo</td>
<td>Available</td>
</tr>
</tbody>
</table>

Support Resources

Commercial Support

TNSR® software is bundled with Netgate TAC Pro support, with TAC Enterprice available for upgrade.

Netgate TAC support options:

<table>
<thead>
<tr>
<th></th>
<th>TAC Pro</th>
<th>TAC Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAC Support Hours</td>
<td>24/7</td>
<td>24/7</td>
</tr>
<tr>
<td>Target Initial Response SLA</td>
<td>24 Hour</td>
<td>4 Hour</td>
</tr>
<tr>
<td>Email / Support Portal</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Telephone Support</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

For more information and purchasing, including the most up-to-date information on available TAC offerings, see: https://www.netgate.com/support.
Community Support

Community support is available through the Netgate Forum.

Additional Resources

Professional Services

Support does not cover more complex tasks such as network design and conversion from other firewalls. These items are offered as professional services and can be purchased and scheduled accordingly.

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

Netgate Training

Netgate training offers training courses for increasing your knowledge of Netgate 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/

Resource Library

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

https://www.netgate.com/resources/

1.2.2 Azure TNSR Instance Setup

This zero-to-ping setup guide will explain how to get started using TNSR to route network traffic in an Azure Virtual Network environment.

Note: Visit the TNSR product page for additional information on purchasing access to TNSR on Azure.

The steps involved are:

Learn the Basics

TNSR utilizes an optimized userspace data plane to forward packets at very high rates. On Azure, TNSR runs on a customized VM instance and is managed by connecting to a command-line interface (CLI) over SSH.

There are many different network designs possible in Azure. This guide assumes a TNSR instance will sit in a Virtual Network connected to a private subnet and a public subnet (one which has access to the Internet).

This guide will show how to bring up a TNSR instance with 3 Virtual Network Interfaces attached:

  Management Interface
  The primary network interface on the instance is used for management of the TNSR instance. This is the interface reached via SSH to connect to the CLI on the TNSR instance. Packets received on
this interface will not be forwarded to another interface. The interface is used for system functions such as DNS resolution and downloading software updates.

The management interface is required but it doesn’t need to have IP Forwarding and Accelerated Networking options set.

**TNSR WAN/Internet Interface**
The TNSR WAN interface is used by TNSR to connect to the Internet. A WAN interface will have a Public IP Address assigned and it will be attached to a subnet that has a route to an Internet Gateway in its Route Table.

**TNSR LAN/Private Interface**
The TNSR LAN interface connects TNSR to a private Subnet in the Virtual Network. The instances in the private subnet do not have their own Public IP Addresses and the Route Table for the subnet does not have a route to an Internet Gateway, but instead has a route to the TNSR LAN interface.

Instances on the private subnet will use TNSR as their gateway to the Internet.

Each of the three network interfaces resides on a distinct subnet.

The examples in this guide use the following configuration:

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Network Address Space</td>
<td>10.5.0.0/16</td>
</tr>
<tr>
<td>WAN Subnet</td>
<td>10.5.0.0/24</td>
</tr>
<tr>
<td>LAN Subnet</td>
<td>10.5.1.0/24</td>
</tr>
<tr>
<td>Management Subnet</td>
<td>10.5.2.0/24</td>
</tr>
</tbody>
</table>

In a real production Virtual Network, the TNSR instance may have more than one WAN interface and/or more than one LAN interface. The concepts covered in this guide can be extended to additional interfaces.

There are some needed flags that cannot be configured using Azure Portal. This guide will cover all necessary steps using **azure-cli**.

**Launch an Instance**

Now launch an instance of TNSR:

1. Install **azure-cli**. Instructions can be found at https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest
2. Login to your Azure account running:
   
   ```
   $ az login
   ```
3. Configure the default location.
   
   ```
   $ az configure --defaults location=centralus
   ```
4. Create a resource group to be used to store all TNSR related objects if it does not already exist.

   ```
   $ az group create -n TNSR-Resource-Group
   ```
5. Create Virtual Network and Subnets.
$ az network vnet create \
    -n TNSR-VNet \
    -g TNSR-Resource-Group \
    --address-prefixes 10.5.0.0/16

$ az network vnet subnet create \
    -g TNSR-Resource-Group \
    --vnet-name TNSR-VNet \
    -n TNSR-WAN-Subnet \
    --address-prefixes 10.5.0.0/24

$ az network vnet subnet create \
    -g TNSR-Resource-Group \
    --vnet-name TNSR-VNet \
    -n TNSR-LAN-Subnet \
    --address-prefixes 10.5.1.0/24

$ az network vnet subnet create \
    -g TNSR-Resource-Group \
    --vnet-name TNSR-VNet \
    -n TNSR-MGMT-Subnet \
    --address-prefixes 10.5.2.0/24

6. Create Public IPs to be used by WAN and Management interfaces.

$ az network public-ip create \
    -g TNSR-Resource-Group \
    -n TNSR-WAN-IP

$ az network public-ip create \
    -g TNSR-Resource-Group \
    -n TNSR-MGMT-IP


$ az network nsg create -n TNSR-MGMT-NSG -g TNSR-Resource-Group
$ az network nsg rule create \
    --name MGMT_Allow_SSH \
    --nsg-name TNSR-MGMT-NSG \
    -g TNSR-Resource-Group \
    --priority 100 \
    --access Allow \
    --destination-port-ranges 22 \
    --direction Inbound \
    --protocol Tcp

8. Create the Management Network Interface.

$ az network nic create \
    -g TNSR-Resource-Group \
    --vnet-name TNSR-VNet \
    --subnet TNSR-MGMT-Subnet \
    -n TNSR-MGMT-nic \

(continues on next page)
9. Create the WAN Network Interface.

```bash
$ az network nic create
  -g TNSR-Resource-Group
  --vnet-name TNSR-VNet
  --subnet TNSR-WAN-Subnet
  -n TNSR-WAN-nic
  --public-ip-address TNSR-WAN-IP
  --ip-forward
  --accelerated-network
```

10. Create the LAN Network Interface.

```bash
$ az network nic create
  -g TNSR-Resource-Group
  --vnet-name TNSR-VNet
  --subnet TNSR-LAN-Subnet
  -n TNSR-LAN-nic
  --ip-forward
  --accelerated-network
```

11. Choose the VM Size to be used. To get a list of sizes that are able to run TNSR, run the following command and export a variable called TNSR_SIZE with it.

```bash
$ az vm list-sizes
  --query 
    "[?numberOfCores >= 4] | 
    [?memoryInMb >= 8192].name | sort(@)"
  --output tsv

$ export TNSR_SIZE=<FILL DESIRED SIZE HERE>

# EXAMPLE:
$ export TNSR_SIZE="Standard_DS4_v2"

12. Choose the TNSR image URN to be used from the list obtained with the following command and export a variable called TNSR_URN with it.

```bash
$ az vm image list
  --publisher Netgate
  --all
  --query 
    "[?contains(offer,'tnsr')].{Sku:sku, Version:version Urn:urn}"
  --output table

$ export TNSR_URN="netgate:netgate-tnsr-azure-fw-vpn-router:netgate-tnsr:20.02.2"

13. Export a variable called TNSR_SSH_KEY containing a path to a valid SSH public key.

```bash
$ export TNSR_SSH_KEY="~/.ssh/id_rsa.pub"

14. Accept Azure Marketplace terms so that the image can be used to create VMs.
**Note:** Previous versions of Azure CLI used the command 

```
$ az vm image accept-terms --urn ${TNSR_URN}
```

---

15. Create a Storage Account.

```
$ az storage account create -n tnsrsa -g TNSR-Resource-Group
```


```
$ az vm create 
  --admin-username tnsr 
  --image ${TNSR_URN} 
  --name TNSR-Instance1 
  --nics TNSR-MGMT-nic TNSR-WAN-nic TNSR-LAN-nic 
  --os-disk-size-gb 20 
  --resource-group TNSR-Resource-Group 
  --size ${TNSR_SIZE} 
  --ssh-key-value ${TNSR_SSH_KEY} 
  --boot-diagnostics tnsrsa
```

### Connect to the Instance

The TNSR instance does not have a default password. SSH connections to this instance require key-based authentication using an SSH key selected when launching the instance.

The default account is named tnsr.

The Management interface Public IP can be discovered from the Azure CLI by running:

```
$ az network public-ip show 
  -n TNSR-MGMT-IP 
  -g TNSR-Resource-Group 
  --query "{ipAddress:ipAddress}" 
  --output tsv
```

To connect from a shell prompt in a Unix/Linux terminal, type the following:

```
$ ssh -i <my_key_file> tnsr@<MGMT_public_ip_addr>
```

Substitute the actual key file name instead of typing `<my_key_file>` and the management interface Public IP Address instead of typing `<mgmt_public_ip_addr>`.

The ssh client will print a warning similar to:

```
The authenticity of host 'x.x.x.x' can't be established.
ECDSA key fingerprint is SHA256:6/LDXVPpD2v6hnWdFHFhWzhKeMcaH4tBgTuDLAa40.
Are you sure you want to continue connecting (yes/no)?
```

This warning only appears the first time connecting using SSH on a given system and user account. Type yes to continue connecting.

If all went well, the TNSR CLI will automatically be launched, resulting in output similar to the following:
Configure Interface Addresses in TNSR

Now that the TNSR CLI is open, start configuring the TNSR instance. First, configure the network interfaces and bring them up.

In TNSR, type `show interface` to view the interface configurations. Here’s an example of what will appear:

```
TNSR-Instance1 tnsr# show interface

Interface: NetVSC2
  Admin status: down
  Link down, 100 Mbit/sec, full duplex
  Link MTU: 9206 bytes
  MAC address: 00:0d:3a:41:f6:b1
  IPv4 Route Table: ipv4-VRF:0
  IPv6 Route Table: ipv6-VRF:0
  counters:
    received: 0 bytes, 0 packets, 0 errors
    transmitted: 0 bytes, 0 packets, 0 errors
    0 drops, 0 punts, 0 rx miss, 0 rx no buffer

Interface: NetVSC3
  Admin status: down
  Link down, 100 Mbit/sec, full duplex
  Link MTU: 9206 bytes
  MAC address: 00:0d:3a:41:f7:20
  IPv4 Route Table: ipv4-VRF:0
  IPv6 Route Table: ipv6-VRF:0
  counters:
    received: 0 bytes, 0 packets, 0 errors
    transmitted: 0 bytes, 0 packets, 0 errors
    0 drops, 0 punts, 0 rx miss, 0 rx no buffer
```

The interface order follows the same order NICs were passed to parameter `--nics` to `az vm create` at `Launch an Instance`. In this guide, the VM has NetVSC2 as WAN and NetVSC3 as LAN.

During the process of creating Network Interfaces, a private IP address was assigned to each interface. We will configure those addresses on the interfaces in TNSR in order to communicate with other instances in the Virtual Network.

Configure WAN interface:

1. Discover assigned IP address in the Azure CLI.
$ az network nic show \
  -g TNSR-Resource-Group \
  -n TNSR-WAN-nic \
  --query "ipConfigurations[].privateIpAddress" \
  -o tsv
10.5.0.4

2. Configure the interface in the TNSR CLI.

TNSR-Instance1 tnsr# configure
TNSR-Instance1 tnsr(config)# interface NetVSC2
TNSR-Instance1 tnsr(config-interface)# ip address 10.5.0.4/24
TNSR-Instance1 tnsr(config-interface)# enable
TNSR-Instance1 tnsr(config-interface)# description TNSR-Instance1 WAN
TNSR-Instance1 tnsr(config-interface)# exit

This sets an address, brings up the interface, and sets a description to serve as a reminder of the interface identity & purpose.

Substitute a different Private IP address/mask and description as needed.

Configure LAN interface:

1. Discover the assigned IP address from the Azure CLI.

   $ az network nic show \
   -g TNSR-Resource-Group \
   -n TNSR-LAN-nic \
   --query "ipConfigurations[].privateIpAddress" \
   -o tsv
10.5.1.4

2. Configure the interface in the TNSR CLI.

   TNSR-Instance1 tnsr(config)# interface NetVSC3
   TNSR-Instance1 tnsr(config-interface)# ip address 10.5.1.4/24
   TNSR-Instance1 tnsr(config-interface)# enable
   TNSR-Instance1 tnsr(config-interface)# description TNSR-Instance1 LAN
   TNSR-Instance1 tnsr(config-interface)# exit

Again, substitute the interface Private IP address/mask and description as needed.

Check the interface status in TNSR again by typing show interface.

TNSR-Instance1 tnsr# show interface

Interface: NetVSC2
   Description: TNSR-Instance1 WAN
   Admin status: up
   Link up, 100 Mbit/sec, full duplex
   Link MTU: 9206 bytes
   MAC address: 00:0d:3a:41:f6:b1
   IPv4 Route Table: ipv4-VRF:0
   IPv4 addresses:
      10.5.0.4/24
The output shows that the interfaces are up and configured, and the counters show that a few packets have been received. It is now possible to verify connectivity with the `ping` command from the TNSR CLI.

```
TNSR-Instance1 tnsr# ping www.netgate.com
PING www.netgate.com (208.123.73.73) 56(84) bytes of data.
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=1 ttl=49 time=19.6 ms
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=2 ttl=49 time=19.5 ms
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=3 ttl=49 time=19.4 ms
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=4 ttl=49 time=20.1 ms
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=5 ttl=49 time=19.5 ms
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=6 ttl=49 time=19.5 ms
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=7 ttl=49 time=19.6 ms
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=8 ttl=49 time=19.6 ms
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=9 ttl=49 time=19.5 ms
64 bytes from www.netgate.com (208.123.73.73): icmp_seq=10 ttl=49 time=19.5 ms
--- www.netgate.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 19.435/19.616/20.136/0.262 ms
```

**Configure Default Route in TNSR**

In order for the TNSR data plane to forward packets outside of the VPC to the Internet, a default route needs to be configured which sets a next hop of the VPC gateway for the WAN subnet using the TNSR CLI.

Configure a default route by typing the commands in TNSR as shown below.

```
TNSR-Instance1 tnsr# configure
TNSR-Instance1 tnsr(config)# route ipv4 table ipv4-VRF:0
TNSR-Instance1 tnsr(config-route-table-v4)# route 0.0.0.0/0
```
Ping TNSR WAN Interface from local Network

The instance should now be reachable via ICMP echo request (ping) using the Public IP Address associated to the TNSR WAN Interface.

To find the Public IP address associated to the TNSR WAN Interface, run:

```bash
$ az network public-ip show \
  -n TNSR-WAN-IP \
  -g TNSR-Resource-Group \
  --query "{ipAddress:ipAddress}" \
  --output tsv
```

Now, try to ping the Public IP Address of the TNSR WAN Interface.

```bash
$ ping -c 5 40.122.49.143
PING 40.122.49.143 (40.122.49.143) 56(84) bytes of data.
64 bytes from 40.122.49.143: icmp_seq=1 ttl=49 time=19.9 ms
64 bytes from 40.122.49.143: icmp_seq=2 ttl=49 time=19.8 ms
64 bytes from 40.122.49.143: icmp_seq=3 ttl=49 time=19.8 ms
64 bytes from 40.122.49.143: icmp_seq=4 ttl=49 time=19.6 ms
64 bytes from 40.122.49.143: icmp_seq=5 ttl=49 time=19.9 ms
--- 40.122.49.143 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 19.649/19.862/19.940/0.140 ms
```

**Warning:** Once the Host OS is capable of reaching the Internet, check for updates (Updating TNSR) before proceeding. This ensures the security and integrity of the router before TNSR interfaces are exposed to the Internet.

References

- Regional Market Availability
- Additional Resources
- Resource Library
Regional Market Availability

The tables below represent the current availability by regional market. If the desired regional market is not listed, refer to the Microsoft Regions availability or submit a support ticket directly to Microsoft Azure.

Table 7: Microsoft Azure Available Regions

<table>
<thead>
<tr>
<th>Market</th>
<th>pfSense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Armenia</td>
<td>Available</td>
</tr>
<tr>
<td>Australia</td>
<td>*</td>
</tr>
<tr>
<td>Austria</td>
<td>Available</td>
</tr>
<tr>
<td>Belarus</td>
<td>Available</td>
</tr>
<tr>
<td>Belgium</td>
<td>Available</td>
</tr>
<tr>
<td>Brazil</td>
<td>Available</td>
</tr>
<tr>
<td>Canada</td>
<td>Available</td>
</tr>
<tr>
<td>Croatia</td>
<td>Available</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Available</td>
</tr>
<tr>
<td>Czechia</td>
<td>Available</td>
</tr>
<tr>
<td>Denmark</td>
<td>Available</td>
</tr>
<tr>
<td>Estonia</td>
<td>Available</td>
</tr>
<tr>
<td>Finland</td>
<td>Available</td>
</tr>
<tr>
<td>France</td>
<td>Available</td>
</tr>
<tr>
<td>Germany</td>
<td>Available</td>
</tr>
<tr>
<td>Greece</td>
<td>Available</td>
</tr>
<tr>
<td>Hungary</td>
<td>Available</td>
</tr>
<tr>
<td>India</td>
<td>Available</td>
</tr>
<tr>
<td>Ireland</td>
<td>Available</td>
</tr>
<tr>
<td>Italy</td>
<td>Available</td>
</tr>
<tr>
<td>Korea</td>
<td>Available</td>
</tr>
<tr>
<td>Latvia</td>
<td>Available</td>
</tr>
<tr>
<td>Liechtenstein</td>
<td>Available</td>
</tr>
<tr>
<td>Lithuania</td>
<td>Available</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Available</td>
</tr>
<tr>
<td>Malta</td>
<td>Available</td>
</tr>
<tr>
<td>Monaco</td>
<td>Available</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Available</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Available</td>
</tr>
<tr>
<td>Norway</td>
<td>Available</td>
</tr>
<tr>
<td>Poland</td>
<td>Available</td>
</tr>
<tr>
<td>Portugal</td>
<td>Available</td>
</tr>
<tr>
<td>Puerto Rico</td>
<td>Available</td>
</tr>
<tr>
<td>Romania</td>
<td>Available</td>
</tr>
<tr>
<td>Russia</td>
<td>Available</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>Available</td>
</tr>
<tr>
<td>Serbia</td>
<td>Available</td>
</tr>
<tr>
<td>Slovakia</td>
<td>Available</td>
</tr>
<tr>
<td>Slovenia</td>
<td>Available</td>
</tr>
<tr>
<td>South Africa</td>
<td>Available</td>
</tr>
<tr>
<td>Spain</td>
<td>Available</td>
</tr>
<tr>
<td>Sweden</td>
<td>Available</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Available</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Available</td>
</tr>
<tr>
<td>Turkey</td>
<td>Available</td>
</tr>
</tbody>
</table>

continues on next page
Table 7 – continued from previous page

<table>
<thead>
<tr>
<th>Market</th>
<th>pfSense</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Arab Emirates</td>
<td>Available</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Available</td>
</tr>
<tr>
<td>United States</td>
<td>Available</td>
</tr>
</tbody>
</table>

* Australia is a Microsoft Managed Country for sales through all customer purchase scenarios except the Enterprise Agreement customer purchase scenario.

### Additional Resources

#### Professional Services

Support does not cover more complex tasks such as network design and conversion from other firewalls. These items are offered as professional services and can be purchased and scheduled accordingly.

[https://www.netgate.com/our-services/professional-services.html](https://www.netgate.com/our-services/professional-services.html)

#### Netgate Training

Netgate training offers training courses for increasing your knowledge of Netgate 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/](https://www.netgate.com/training/)

#### Resource Library

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

[https://www.netgate.com/resources/](https://www.netgate.com/resources/)

### 1.3 Virtual Machines

A TNSR software Bare Metal Image is available and will run in most virtual x86 environments.

- **VMware** - vSphere/ESXi 6.0 and later, running VMXNET3 virtual network adapters.

  **Note:** VMware VMXNET3 interfaces are not currently compatible with VRRP. The VMXNET3 interface driver does not support setting virtual MAC addresses, which is required by VRRP.

  **Warning:** Secure boot is not compatible with TNSR, it prevents interfaces from being added to the dataplane when it is enabled. If a VMware virtual machine has **Firmware** set to **EFI** under **VM Options > Boot Options**, then **Enable UEFI secure boot** must be **unchecked**.

- **KVM** - Kernel Virtual Machine on Linux.
• **virtio-net** - Paravirtualized network adapter used by other hypervisors such as QEMU and VirtualBox.

### 1.3.1 Using TNSR on KVM

TNSR can be run on a Linux Kernel Virtual Machine (KVM) hypervisor host. The advice on this page is specifically geared toward KVM managed by *libvirt*.

#### Installing TNSR on KVM

When creating the virtual machine, use the requirements on *Supported Platforms* as a guide for determining configuration parameters before starting. For example:

- Number of CPUs, Cores, and their topology
- Amount of RAM
- Storage size
- Network connectivity type, number of interfaces, networks to which interfaces connect

#### Creating a VM

Before starting, obtain the installation ISO and place it in a known location.

The following command will create a new virtual machine from the KVM CLI with the following configuration:

- 2 virtual CPUs (1 socket, 2 cores per CPU, 1 thread per core)
  - Set CPU to host or qemu64,+ssse3,+sse4.1,+sse4.2,+x2apic
- 4GB RAM
- A new 32GB virtio disk named `tnsr.qcow2`
- 3 virtio-based network interfaces

```
# virt-install --name TNSR --vcpus=2,sockets=1,cores=2,threads=1 \
   --os-type linux --os-variant ubuntu20.04 --cpu host --ram 4096 \
   --disk /var/lib/libvirt/images/tnsr.qcow2,size=32,device=disk,bus=virtio \n   --network=default,model=virtio --network bridge=br0,model=virtio \
   --network bridge=br1,model=virtio \
   --nographics --noautoconsole \
   --location /root/TNSR-Ubuntu.iso,kernel=casper/vmlinuz,initrd=casper/\n   --initrd \n   --extra-args 'console=ttyS0,115200n8 quiet fsck.mode=skip \n   network-config=disabled autoinstall ds=nocloud;s=/cdrom/server/
```

**Note:** Replace the parameters as needed to conform to the local KVM environment. In particular, the `--disk` path, ISO `--location` path, and bridge device or network names will likely be different.

Access the management console with the following command:

```
# virsh console TNSR
```
From the console, follow the standard TNSR installation procedure and the VM will shut down afterward. Start it again and reconnect to the console:

```bash
# virsh start TNSR
# virsh console TNSR
```

KVM Frontends/GUIs can also accomplish the same goal in different ways. Use whichever method is preferred by the hypervisor administrator.

**KVM Optimization**

Virtio interfaces use tap as a backend, which requires a memcpy() of each packet forwarded. Due to this design, the stock configuration can result in poor performance. The tuning suggestions in this section will help obtain higher performance in these environments.

**Note:** Though these suggested changes have been found to improve performance in testing, every installation and workload is different. Real-world results may vary depending on the environment. Generally speaking, values should only be changed from the defaults in cases where performance is lower than expected.

- Set the vhost backend driver `rx_queue_size` and `tx_queue_size` values to 1024 instead of the default 256.
  To set these values in the libvirt xml configuration for a VM, see Changing VM Parameters.
- Increase the number of queues in the vhost backend driver configuration, especially if TNSR is configured to use worker threads. This information is also in the section linked above.
- Try using SR-IOV VFIs instead of Virtio interfaces.
- Try using a DPDK accelerated OpenVSwitch (OVS-DPDK) instead of a standard linux bridge.

**Changing VM Parameters**

Some values must be changed by editing the VM settings XML directly. This includes the receive and transmit ring queue sizes and the number of queues.

When setting the receive and transmit ring queue sizes, keep in mind that some environments impose specific requirements on the values. For example, they may only work with certain drivers, or may have value restrictions such as being a power of 2 (256, 512, 1024, etc.).

To edit the VM XML parameters, use the following command:

```bash
# virsh edit TNSR
[...]
```

Find the `interface` tag(s) and the `driver` tags inside. In the `driver` tag, edit or add the desired attributes and values. For example, to set 5 queues, and 1024 size transmit and receive ring queue sizes:

```xml
<interface [...]> [...]
  <driver name='vhost' txmode='iothread' iodev='on' event_idx='off' queues='5' rx_queue_size='1024' tx_queue_size='1024'> [...]
</driver>
[...]
</interface>
```
Start the VM, and check the `qemu` command line, which should contain `rx_queue_size=1024`, `tx_queue_size=1024`.

From within the VM, at a shell prompt, confirm the ring queue sizes:

```
# ethtool -g eth0
Ring parameters for eth0:
Pre-set maximums:
RX: 1024
[...]
TX: 1024
Current hardware settings:
RX: 1024
[...]
TX: 1024
[...]
```

If the number of queues was changed, confirm that as well:

```
# ethtool -l eth0
Channel parameters for eth0:
Pre-set maximums:
[...]
Combined: 5
[...]
```

See also:

For more details, see:

- The libvirt-users mailing list, including this post describing the process.
- The libvirt XML format documentation

### 1.4 Recommended Components

TNSR runs on Linux for x86 processors. For best results in data center environments, the following CPUs are recommended:

- Intel Xeon Processor E3 Families (v2, v3, v4, v5, v6, and v7)
- Intel Xeon Processor E5 Families (v2, v3, v4, v5, v6, and v7)
- Intel Xeon Processor E7 Families (v2, v3, v4, v5, v6, and v7)
- Intel Xeon Scalable Processors
- Intel Xeon D Processors
- Intel Atom C2000 & C3000 Processors
Note: TNSR can utilize accelerator technology, such as Intel QuickAssist Technology (QAT) featured in the Intel Atom C2000 and C3000 processors, and the Netgate CPIC-8955 Cryptographic Accelerator Card.

Network Interface Card (NIC) support in TNSR is provided by drivers in the underlying Linux operating system. The following NIC drivers have been tested by Netgate:

**igb**
- NICs based on the following Intel Gigabit Ethernet controllers:
  - 82575/6, 82580, I350, I354, I210/211

**ixgbe**
- NICs based on the following Intel 10 Gigabit Ethernet controllers:
  - 82598/9, X520, X540, X550, X553, X552/X557-A

**i40e**
- NICs based on the following Intel 10/40 Gigabit Ethernet controllers:
  - X710, XL710, XXV710

**Note:** These NICs require a DPDK compatible firmware version which is listed on the DPDK website.

Check the TNSR release notes to see which version of DPDK is present in TNSR. Utilities to update the NVM firmware on these NICs can be downloaded from Intel.

**mlx5**
- NICs based on the following Mellanox 10/25/40/50/100 Gigabit Ethernet controllers:
  - ConnectX-4, ConnectX-4 Lx, ConnectX-5
CHAPTER TWO

UNTESTED PLATFORMS

The best practice is to use a platform tested by Netgate. That said, the underlying components may support additional hardware that has not been tested by Netgate nor confirmed to run TNSR software successfully.

Netgate customers are often on the cutting edge of technology, so they may encounter systems and components that work with TNSR before Netgate has an opportunity to test them.

**Warning:** Netgate cannot offer any assurance that untested platforms will be compatible with TNSR software or perform at acceptable levels.

Hardware support is primarily determined by The Data Plane Development Kit (DPDK) and Vector Packet Processing (VPP) open source projects which are core parts of TNSR. Additionally, the underlying operating system drivers must support the hardware (i.e. boot, load the OS, etc.) and network interfaces used for host management. TNSR may run on a system if these components support the hardware in question, but experiences will vary.

For the latest information on hardware supported by DPDK and VPP, check here:

- https://core.dpdk.org/supported/
- http://doc.dpdk.org/guides/nics/overview.html#id1