Secure Router Manual

Amazon AWS

Nov 09, 2020

CONTENTS

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

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

The steps involved are:

CHAPTER

ONE

LEARN THE BASICS

TNSR utilizes an optimized userspace data plane to forward packets at very high rates. On AWS, TNSR runs on a customized CentOS 7 Linux 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 1: Example AWS Network Configuration

Item	Value
VPC Address Space	10.5.0.0/16
WAN Subnet	10.5.0.0/24
LAN Subnet	10.5.1.0/24
Management Subnet	10.5.2.0/24

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.

CHAPTER

TWO

LAUNCH AN INSTANCE

Now launch an instance of TNSR:

1. Navigate to https://console.aws.amazon.com/ec2/
2. Click **Instances**
3. Click **Launch Instance** to enter the **Launch Instance Wizard**
4. Click the **AWS Marketplace** heading
5. Type `Netgate` in the search box and press `Enter`
6. Find the entry for TNSR and click **Select**
7. Click **Continue** on the information page
8. Choose an **Instance Type**, then click **Next**

   Note: 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/
   - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#AvailableIpPerENI

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

   ---

9. Configure Instance Details:
   - Select the VPC in which to launch the instance
   - Under **Network Interfaces**:
     - Select the **Management subnet** as the subnet for the **eth0** interface
     - Click the **Add Device** button
     - Select the **WAN subnet** as the subnet for the **eth1** interface

   Only two Network Interfaces may be added to an instance at launch time. The LAN interface can be added after the instance is launched.

   Click **Next** after completing the choices

10. Add storage if this instance will require more than the default 10GB disk, then click **Next**
11. Add **Tags** to identify this instance if desired, then click **Next**
12. Configure Security Group

    Default rules should appear to allow SSH and ICMP. These rules can be used to create a new security group, and to add access for other ports if needed.

    > **Warning:** We strongly recommend that the allowed **Source** be limited to a specific address or network that will be used connect to the TNSR instance.

    Give the security group a name such as "TNSR management".
13. Verify the settings selected in earlier steps, then click **Launch**

    Select an ssh key or create a new key in the popup. Click **Launch Instances**

CHAPTER

THREE

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 we recommend entering **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

CHAPTER

FOUR

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 here https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#change_source_dest_check

CHAPTER

FIVE

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

CHAPTER

SIX

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`.

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/LDXVPpD2v6hnWdFHFWZhkCbSpMcaH4tBgTuDLAa40.
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#
```

CHAPTER

SEVEN

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
```

(continues on next page)

(continued from previous page)

```
      0 drops, 0 punts, 0 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
    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. We will 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
tnsr(config-interface)# exit
tnsr(config)# exit
```

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.
```

(continues on next page)

(continued from previous page)

```
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
64 bytes from 10.5.0.1: icmp_seq=3 ttl=64 time=0.220 ms

--- 10.5.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.096/0.182/0.231/0.062 ms

tnsr# ping 10.5.1.1 source 10.5.1.218 count 3
PING 10.5.1.1 (10.5.1.1) 56(84) bytes of data.
64 bytes from 10.5.1.1: icmp_seq=1 ttl=64 time=0.071 ms
64 bytes from 10.5.1.1: icmp_seq=2 ttl=64 time=0.123 ms
64 bytes from 10.5.1.1: icmp_seq=3 ttl=64 time=0.157 ms

--- 10.5.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.071/0.117/0.157/0.035 ms
```

7.1 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

CHAPTER

EIGHT

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#
```

CHAPTER

NINE

PING TNSR WAN INTERFACE FROM YOUR 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*
- *Additional Resources*
- Resource Library

CHAPTER

TEN

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 1: AWS Available Regions

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

CHAPTER

ELEVEN

ADDITIONAL RESOURCES

11.1 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

11.2 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/

11.3 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/