Configure Service-Side Static NAT on a Cisco IOS XE SD-WAN Router

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Network Diagram

Configuration

- cEdge Configuration
  - Via CLI
  - Via vManage feature template
- Centralized Data Policy

Verify

Troubleshoot

Related Information

Introduction

This document describes the configuration to perform a static NAT to and from service side VRF on a Cisco IOS-XE® SD-WAN Router.

Prerequisites

Cisco IOS-XE SD-WAN devices on version 17.3.1a or later must be used.

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Network Address Translation (NAT)

Components Used

The information in this document is based on these software and hardware versions.

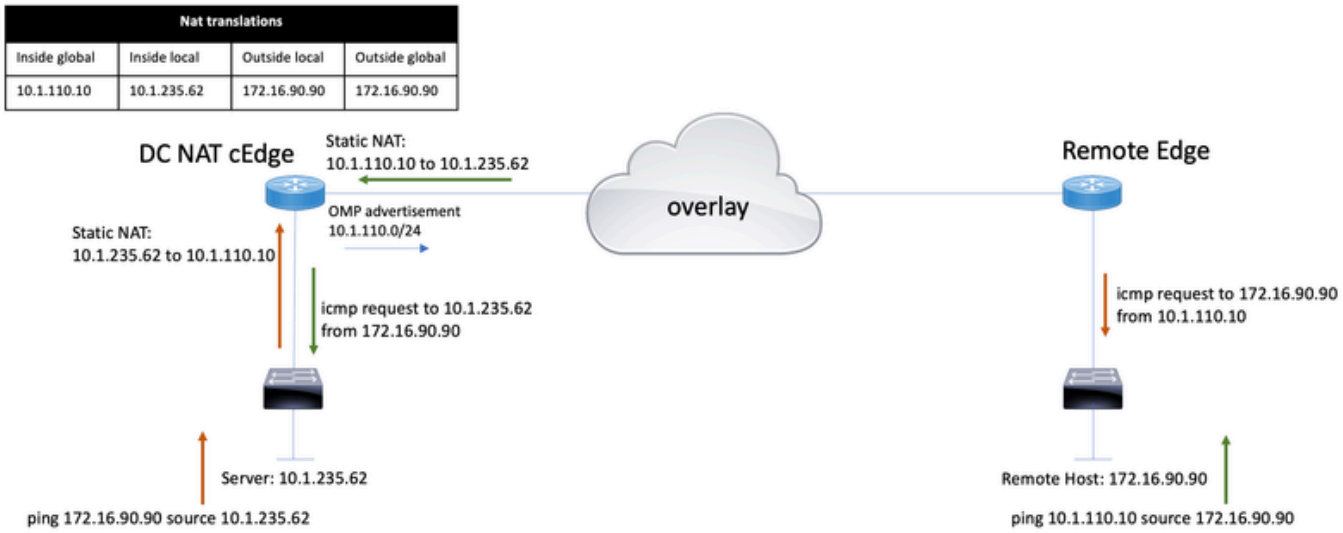
- ISR4451-X/K9 version 17.6.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Network Diagram

In order to configure the Service Static NAT described in this document, this topology is used.



The 10.1.235.0/24 subnet is private and local to the DC site. This subnet is not advertised into Overlay Management Protocol (OMP). In order for the servers to have communication, these are natted statically to the 10.1.110.0/24 subnet.

- When server 10.1.235.62 initiates the communication to 172.16.90.90, cEdge needs to NAT 10.1.235.62 to 10.1.110.10.
- When the host 172.16.90.90 needs to communicate to the server, it does the request to 10.1.110.10, and the cEdge needs to translate the destination IP to 10.1.235.62.

Configuration

cEdge Configuration

This configuration can be performed through the router CLI or through a vManage feature template.

Via CLI

Configure the NAT Pool:

```
ip nat pool natpool10 10.1.110.1 10.1.110.253 prefix-length 24
```

Configure an inside static NAT global pool:

```
ip nat inside source list global-list pool natpool10 vrf 10 match-in-vrf
```

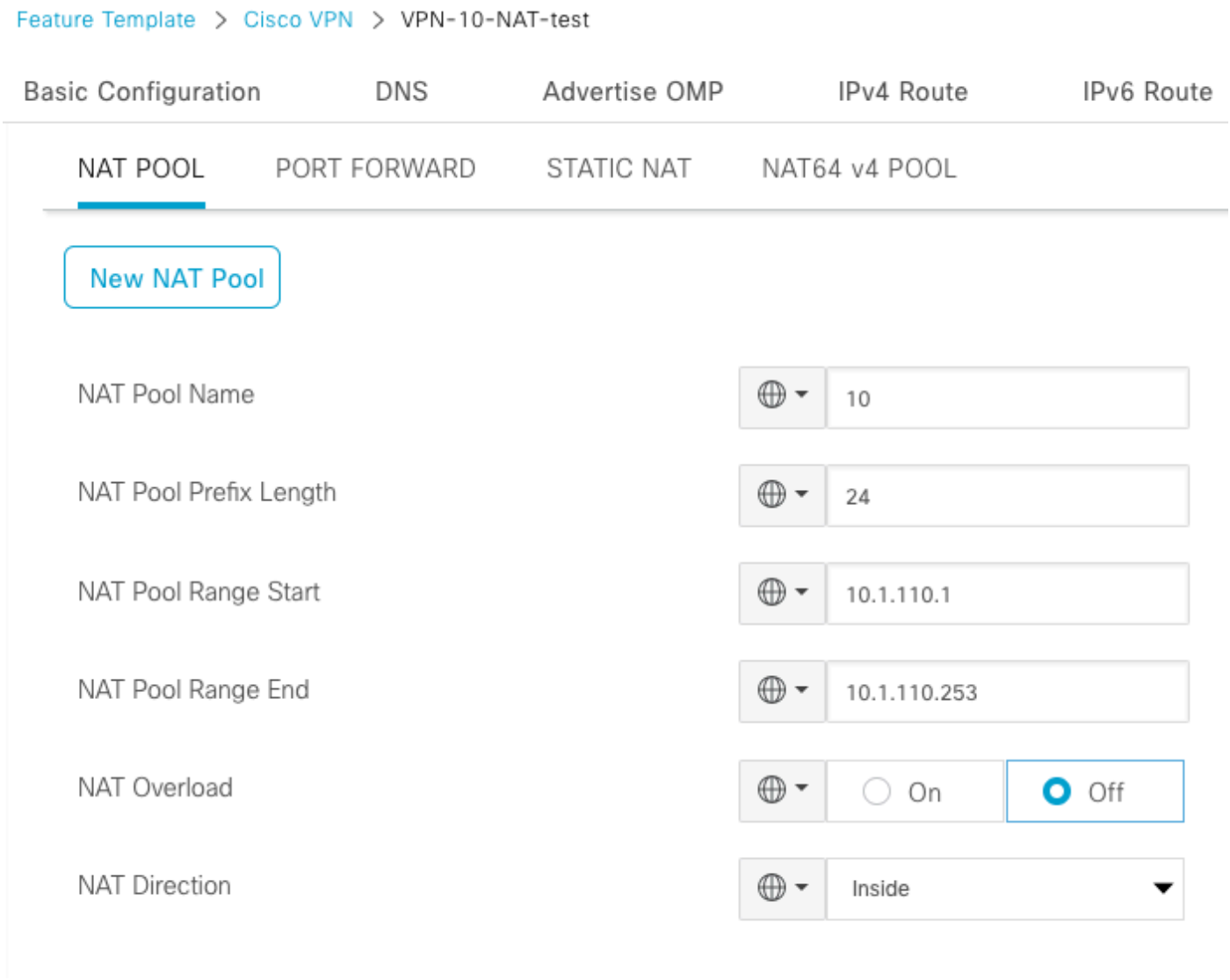
Configure the static NAT entry:

```
ip nat inside source static 10.1.235.62 10.1.110.10 vrf 10 match-in-vrf pool natpool10
```

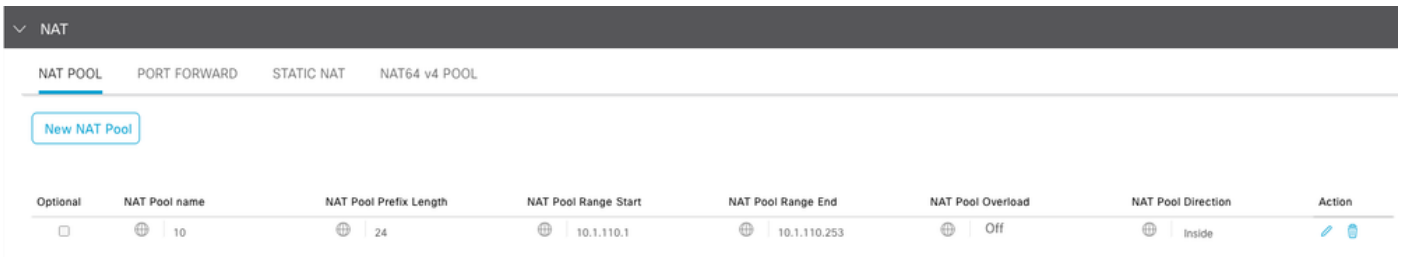
Via vManage feature template

In the service VPN feature template, navigate to **NAT section > NAT Pool** and click **New NAT Pool**.

Fill in the variables and click **Add** when finished:

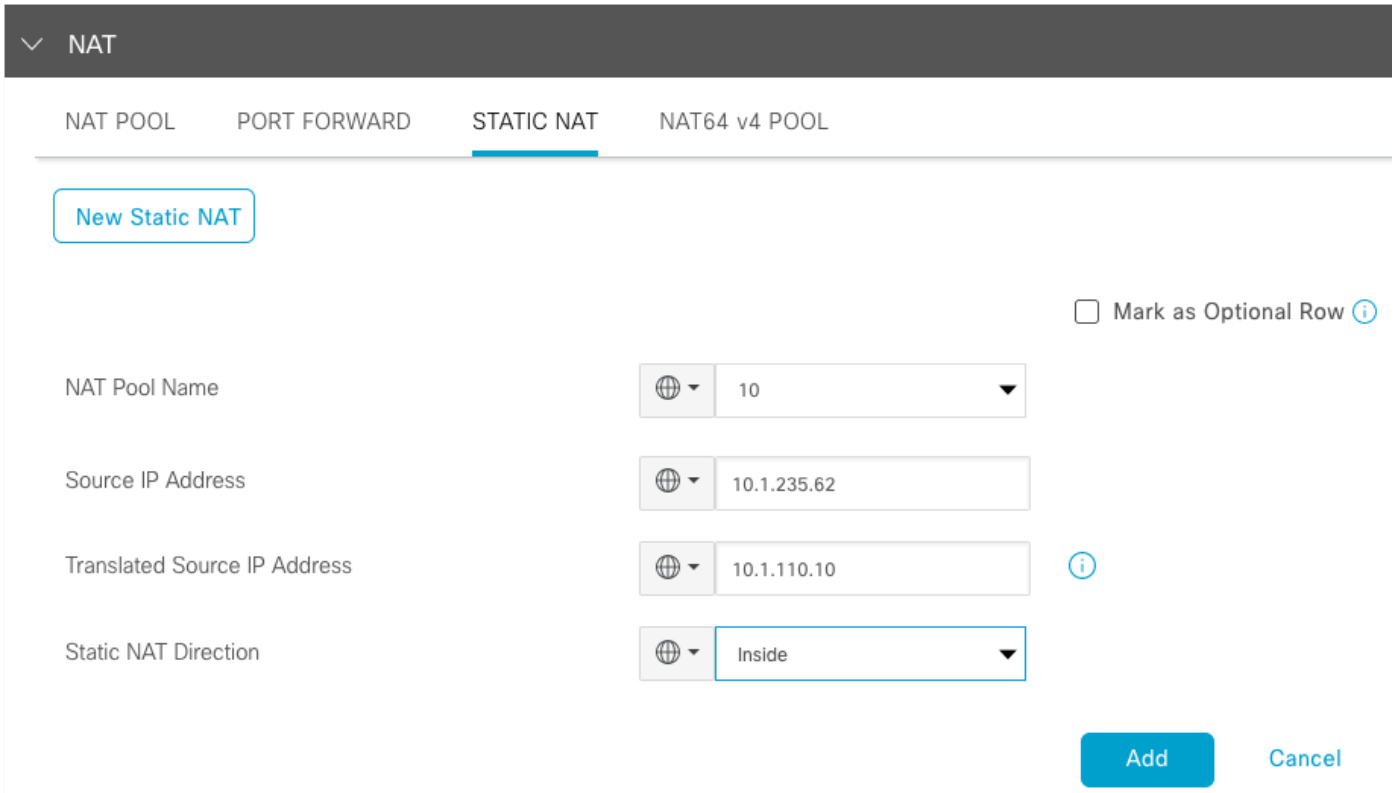


Verify the Pool is created as follows:



Once Pool is created, navigate to **Static NAT** and click the button **New Static NAT**.

Fill in the variables and click **Add** once finished:



Centralized Data Policy

A centralized data policy is needed to direct the data traffic with the desired prefixes to the service-side NAT.

Define VPN and site list:

```
policy
 lists
  vpn-list VPN-10
   vpn 10
  !
  site-list CEDGE
   site-id 30
  !
```

Define the first sequence for the inside to outside translation:

<#root>

```
data-policy _VPN-10_Data_NAT_cEdge
 vpn-list VPN-10
  sequence 1
   match
```

```
source-ip 10.1.235.62/32


   !
   action accept
    count nat_cedge_-1665659624
    nat pool 10
   !
  !
```

The next sequence is used for the translation of the destination address. It is used when traffic is initiated from outside to inside:

<#root>

```
  sequence 11
   match


 destination-ip 10.1.110.10/32


   !
   action accept
    count nat_cedge_out2in_-1665659624
    nat pool 10
   !
  !
  default-action accept
 !
!
```

Apply the policy in all directions:

```
apply-policy
 site-list CEDGE
   data-policy _VPN-10_Data_NAT_cEdge all
```

Verify

Verify the state of the NAT configuration with the verification commands.

```
show sdwan policy from-vsmart
show ip nat translations
sdwan policy data-policy-filter
```

Ping from server 10.1.235.62 to host 172.16.90.90 test:

```
cEdge#show ip nat translations
Pro   Inside global   Inside local   Outside local   Outside global
---   10.1.110.10     10.1.235.62    ---             ---
icmp  10.1.110.10:0   10.1.235.62:0  172.16.90.90:0   172.16.90.90:0
Total number of translations: 2
```

Ping from host 10.90.90.90 to server 10.1.110.10 test:

```
cEdge#show ip nat translations
Pro   Inside global     Inside local     Outside local     Outside global
---   10.1.110.10       10.1.235.62      ---               ---
icmp  10.1.110.10:8299  10.1.235.62:8299 172.16.90.90:8299  172.16.90.90:8299
Total number of translations: 2
```

Troubleshoot

Check if the packets increased on the data policy counters:

<#root>

```
cEdge#show sdwan policy data-policy-filter
data-policy-filter _VPN-10_Data_NAT_cEdge
 data-policy-vpnlist VPN-10
  data-policy-counter default_action_count
   packets 1412
   bytes 109382
```

data-policy-counter nat_cedge_-1665659624

packets 154

bytes 16852

data-policy-counter nat_cedge_out2in_-1665659624

packets 7

bytes 886

Related Information

- Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE Release 17.x