

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

Contents

[Introduction](#)

[Prerequisites](#)

[Recommendations](#)

[Components Used](#)

[Background](#)

[Configuration](#)

[Verification](#)

Introduction

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

Prerequisites

Cisco IOS-XE SD-WAN devices on version 17.2.1 or later code must be used.

Recommendations

Cisco recommends that you have knowledge of these topics:

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

Components Used

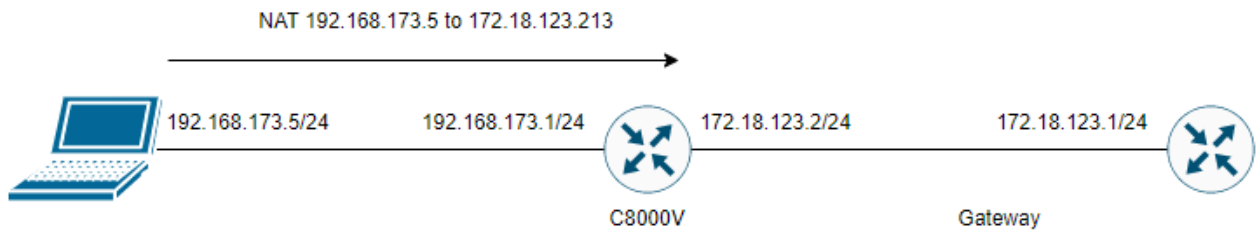
The information in this document is based on these software and hardware versions.

- C8000V version 17.6.3a

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

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



Configuration

This configuration can be performed through the router CLI or through a vManage CLI Add-On template.

NAT overload configuration is required

```
ip nat inside source list nat-dia-vpn-hop-access-list interface <WAN Interface> overload
```

Configure a static NAT statement

```
ip nat inside source static <inside local IP of server> <inside global IP of server> vrf <vrf server is in> egress-interface <WAN Interface>
```

Configure a route in Virtual Routing and Forwarding(VRF) routing traffic back to the global VRF for egress traffic

```
ip nat route vrf <vrf of server> <inside global IP of server> 255.255.255.255 global
```

Enable NAT on the interface:

```
interface <WAN Interface> ip nat outside
```

Example configuration:

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
ip nat inside source static 192.168.173.5 172.18.123.213 vrf 10 egress-interface
GigabitEthernet1
ip nat route vrf 10 172.18.123.213 255.255.255.255 global
interface GigabitEthernet1
ip nat outside
```

Verification

Once the configuration is completed, the functionality can be verified with the command **show ip nat translations**.

```
cEdge#sh ip nat translations Pro Inside global Inside local Outside local Outside global --- 172.18.123.213 192.168.173.5 --- --- tcp
172.18.123.213:22 192.168.173.5:22 172.18.123.224:50708 172.18.123.224:50708 tcp 172.18.123.213:53496
192.168.173.5:53496 10.165.200.226:443 10.165.200.226:443
```

In the output above, it is seen that there are now successful NAT translations on the router. To

test, an ssh session was performed to the PC itself from another device in the transport vrf.