Service Side Destination Based NAT on vEdge Router

Contents

Introduction

This document describes how to configure destination-based Network Address Translation (NAT) in service VPN on vEdge router.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco SD-WAN.

Components Used

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

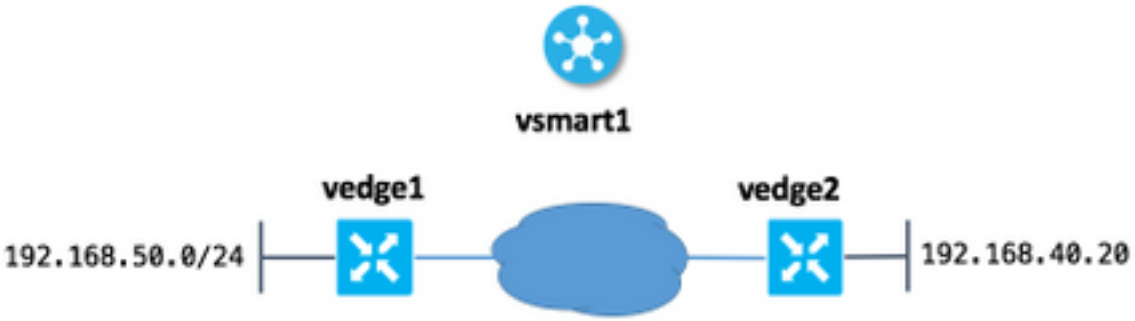
- vEdge Routers
- vSmart Controller with an 18.3 software version.

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.

Configure

Network Diagram

The network diagram is shown here.



The main idea here that users of site 50 (vedge1) can reach to host 192.168.40.20 at another side via IP-address 192.168.140.20.

This is analog of this IOS configuration statement:

```
ip nat outside source static 192.168.40.20 192.168.140.20
```

Configurations

1. Configure the NAT pool on vEdge at site 50.

```
vedge1#show running-config vpn 40 interface natpool31
vpn 40
 interface natpool31
  ip address 192.168.140.5/32
  nat
   static source-ip 192.168.40.20 translate-ip 192.168.140.20 outside
  !
  no shutdown
 !
!
```

2. Configure and apply data policy on vSmart.

```
vsmart1# show running-config policy data-policy DNAT
policy
 data-policy DNAT
  vpn-list CORP
   sequence 10
    match
     destination-ip 192.168.140.20/32
    !
    action accept
     nat pool 31
    !
   !
   default-action accept
  !
 !
!

vsmart1# show running-config apply-policy site-list site_50
apply-policy
 site-list site_50
  data-policy DNAT all
```

```
 !
!
```

Verify

1. Check that translation is there in a corresponding service VPN.

```
vedge1# show ip nat interface nat-vpn 40

                                                                                FIB
NUMBER
                                                                FILTER  FILTER
IP
VPN  IFNAME     MAP TYPE              FILTER TYPE               COUNT   COUNT   IP
POOLS
-------------------------------------------------------------------------------------------------
---------
40   natpool31  endpoint-independent  address-port-restricted  0       0       192.168.140.5/32
1
```

2. Check that policy applied to vEdge from vSmart.

```
vedge1# show policy from-vsmart
from-vsmart data-policy ENK_NAT
 direction all
 vpn-list CORP
  sequence 10
   match
    destination-ip 192.168.140.20/32
   action accept
    nat pool 31
  default-action accept
from-vsmart lists vpn-list CORP
 vpn 40
```

Troubleshoot

If destination-based NAT does not work, then the important thing here is that you must ensure that the IP address of the NAT pool is reachable from the destination host. This is important because as per vEdge router destination-based NAT implementation source IP address is also NATed to the IP address of the pool.
So, for example, based on sample config destination address 192.168.140.20 is replaced with real IP-address 192.168.40.20, but the address of the host from 192.168.50.0/24 subnet at site 50 is also NATed to 192.168.140.5, hence you must have a route back to this address anyway or reply packets won't reach source host (requester). This can be achieved with the advertisement for the NAT pool subnet. In this example, the subnet consists of just one address and advertised via Overlay Management Protocol (OMP).

Here is you can check that route is presented on vEdge1 at the remote site:

```
vedge2# show ip routes vpn 40 omp | i 192.168.140.5
40     192.168.140.5/32    omp              -         -           -                -
192.168.30.5     mpls             ipsec  F,S
```