

Service-Side NAT

Table 1: Feature History

Feature Name	Release Information	Description
Service-Side NAT on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature allows you to configure inside and outside NAT on data traffic traveling to and from the service-side hosts of the network overlay. The service-side NAT configuration allows you to translate the source IP addresses for data traffic from service-side hosts to the overlay and traffic from the overlay to service-side hosts.
Intra-VPN Service-Side NAT Support	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	Intra-VPN allows service-side LAN interfaces to communicate with other service-side LAN interfaces within the same VPN. Configure the **ip nat outside** command on the LAN interface for which you require translation of the source IP addresses to the outside local addresses. You can apply static or dynamic NAT rules for packets to be routed from other LAN interfaces to the interface configured as the outside interface. You can configure intra-VPN service-side NAT using a device CLI template or a CLI add-on template.

Feature Name	Release Information	Description
Service-Side Conditional Static NAT Support	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This feature allows you to translate the same source IP address to different IP addresses based on the destination IP addresses. You can configure service-side conditional static NAT using a device CLI.
Service-Side Static Network NAT Support	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature supports configuration of service-side static NAT for a subnet. Instead of configuring multiple static NAT pools, you can configure a single static NAT pool for an entire subnet. You can configure service-side static network NAT using Cisco SD-WAN Manager or a device CLI template.
Application-Level Gateway (ALG) in Service-Side NAT	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Use an application-level gateway (ALG) to interpret the application-layer protocol and perform service-side NAT translations for FTP protocol.

- Information About Service-Side NAT, on page 2
- Traffic Flows for Service-Side NAT, on page 4
- Restrictions for Service-Side NAT, on page 4
- Configure Service-Side NAT, on page 5
- Configure Service-Side NAT Using the CLI, on page 10
- Intra-VPN Service-Side NAT, on page 15
- Service-Side Conditional Static NAT, on page 19
- Service-Side Static Network NAT, on page 21
- Application-Level Gateways with Service-Side NAT, on page 23

Information About Service-Side NAT

On a Cisco IOS XE Catalyst SD-WAN device, you can configure NAT on the service-side of the device so that data traffic is NATed before entering the overlay tunnel that is located in the transport VPN. The service-side NAT masks the IP address of data traffic it receives.

You can configure both dynamic and 1:1 static NAT on the service-side of a device. To do this, you configure a NAT pool interface within a service VPN on the device, and then you configure a centralized data policy on the Cisco Catalyst SD-WAN Controller. The policy directs data traffic with the desired prefixes to the service-side NAT. You configure either dynamic NAT or static NAT on the desired NAT pool interface.

When service-side NAT is enabled, all matching prefixes in VPN 1 are directed to the NAT pool interface. This traffic is NATed, with the NAT swapping out the service-side IP address and replacing it with its NAT pool IP address. The packet then gets forwarded to its destination.

You can configure NAT for data that enters or exits the service-side of the network. The service-side NAT translates data traffic, of inside and outside host addresses, that match a configured centralized data policy.

Inside Source Address Translation

When service-side or LAN-side hosts send traffic to remote branches, the inside address translation services allow the source IP address (inside host) translation. This translation occurs before the data traffic is sent out to the overlay tunnels. The NAT inside pool and the inside static NAT addresses are redistributed to the overlay. These addresses are advertised to all the remote branches using the Overlay Management Protocol (OMP). Thus, the remote host is aware of the path to reach inside hosts.

For inside-address translation, the data traffic from service-side is matched with the centralized data policy match condition for dynamic NAT. If the source IP address satisfies the match condition, the data traverses the NAT configured on the service VPN before entering the remote edge router through the overlay. Address translation occurs on the tunnel egress interface. In releases before Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier up to Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, the static-inside NAT does not need a match condition in a centralized data policy. The static translation occurs if the source IP address matches the configured IP address for static NAT.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you must map static NAT to a pool and static NAT is applied to the traffic if there is a data policy match.

Outside Source Address Translation

When the traffic from a remote site traverses through the overlay tunnels, the outside address translation service translates the remote host source IP address (outside host). The translation occurs before the traffic is sent to the LAN (VPN) side of the network. If route redistribution is configured, the NAT outside pool address or routes are redistributed to the LAN side of the network through Open Shortest Path First (OSPF) or other protocols. Thus, the inside host is aware of the path to reach remote hosts.

In releases before Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier up to Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, both inside and outside service-side NAT must be a dynamic NAT configuration. You can also configure 1:1 static NAT mapping for both inside and outside address translation.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you must configure a NAT pool action for static NAT as well, using a centralized data policy in order to operate for both source and destination directions.

Note Configure dynamic NAT before you configure static NAT.

Data Policy for Service-Side NAT

To enable NAT on the Cisco IOS XE Catalyst SD-WAN devices, configure a centralized data policy for static and dynamic NAT. A data policy provides the match criteria and NAT pool action for dynamic NAT.

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can create a data policy to configure match criteria and a NAT pool action for static NAT.

Benefits of Service-Side NAT

- Provides translation of source IPv4 addresses to destination IPv4 addresses
- Maps a public IPv4 address to a private source IPv4 address
- Provides a way for service providers to implement a seamless transition to IPv6

Traffic Flows for Service-Side NAT

The following are the two data traffic flows for service-side NAT:

- Source translation for traffic from service-side of the network destined to the remote edge through the overlay network
- Source translation for traffic destined to the service-side of the network from the remote edge through the overlay network

NAT Feature Invocation Array (FIA) from service-side—When the traffic is from the service-VPN that is destined to the remote edge through the tunnel, NAT FIA is enabled on the egress interface, which is the tunnel interface. The data policy direction is configured as from-service.

NAT FIA from-tunnel—When the traffic is from the remote edge that comes through the tunnel and reaches the service VPN, NAT FIA is enabled on the egress interface, which is the service VPN LAN interface. The data policy direction is configured as from-tunnel.

When the data policy direction is configured as all (all directions), NAT FIA is enabled on service VPN interfaces and tunnel interfaces.

Note The IP addresses of a centralized data policy and static NAT source IP address must not overlap in Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier releases up to Cisco IOS XE Catalyst SD-WAN Release 17.3.1a. The centralized data policy must be clearly defined so that there are no overlapping traffic match conditions.

Restrictions for Service-Side NAT

- Only NAT pool translations are supported.
- Translations between different VRFs are not supported.
- In Cisco SD-WAN Manager, you can configure a maximum of 31 pools.

- Specify the NAT pool name as **natpool** *natpool-number*, where *natpool-number* must match the NAT pool value specified in the data policy.

  Example: `natpool10`

- In Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, and Cisco IOS XE Catalyst SD-WAN Release 17.3.2, a static NAT address must not be shared in pool addresses.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the static NAT address may belong to the configured NAT pool address list, if it is used along with a data policy.
- A data policy and dynamic NAT pool must be defined for static NAT for a VRF.
- IPv4 translations for NAT64 are not supported.
- Each service VPN must have a unique NAT pool number.
- NAT entries cannot be edited after they are first created.

Configure Service-Side NAT

Workflow for Configuring Service-Side NAT

1. Configure a centralized data policy for the Cisco Catalyst SD-WAN Controller to include a NAT pool number and action. The direction of the centralized data policy for NAT inside must be **from-service**. The direction of the policy for NAT outside must be **from-tunnel**.
2. Configure a dynamic NAT pool number using a **Cisco VPN** template, which is a service-side VPN.
3. Configure dynamic NAT mappings using a **Cisco VPN** template.
4. (Optional) Configure a static NAT mapping using a **Cisco VPN** template.

   Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can configure a NAT pool for static NAT and create a data policy to provide match criteria and a NAT pool action for static NAT.

   For more information on configuring service-side static NAT, see Configure Service-Side Static NAT.
5. For NAT inside, the NAT pool subnet and static NAT translation of IP addresses are automatically advertised into OMP. For NAT outside, you can manually configure redistribution of the NAT pool subnet and static NAT translation of IPv4 addresses to the service-side protocols.

Note If the data policy action is configured for VPN 0, the action is configured for DIA traffic. If the data policy action is configured for any of the service VPNs (example: VPN 1), which includes a NAT pool configuration, the action is for service-side NAT.

Create and Apply a Centralized Data Policy for Service-Side NAT

A centralized data policy is a policy that is configured on a Cisco Catalyst SD-WAN Controller and that affects data traffic being transmitted between the routers on the Cisco Catalyst SD-WAN overlay network.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. Click **Add Policy**.

   The policy configuration wizard opens. For more information on creating a centralized data policy, see Configure Centralized Policies Using Cisco SD-WAN Manager.
4. Create policy lists.

   For more information on configuring groups of interest, see Configure Groups of Interest for Centralized Policy.
5. Configure traffic rules.

   For more information on configuring traffic rules, see Configure Traffic Rules.
6. Apply policies to sites and VPNs.

   For more information on applying policies to sites and VPNs, see Apply Policies to Sites and VPNs.

   Choose the direction for applying the policy as **All**, **From Tunnel**, or **From Service**.

   Table 2: Dynamic and Static NAT Application

NAT Configuration	Data-Policy Direction
Dynamic NAT Inside only (NAT Pool)	From-service
Dynamic NAT Outside only (NAT Pool)	From-tunnel
Dynamic NAT Inside (NAT Pool) + Static NAT Inside only	From-service
Dynamic NAT Inside (NAT Pool) + Static Port Forwarding only	From-service
Dynamic NAT Outside (NAT Pool) + Static NAT Outside only	From-tunnel
Two or more of above combinations	all

7. Activate the policy.

   For more information on activating a policy, see Activate a Centralized Data Policy.

Configure Service-Side Dynamic NAT

Before You Begin

1. Configure a centralized data policy for the Cisco Catalyst SD-WAN Controller to include a NAT pool number and an action.
2. Create a new **Cisco VPN** template or edit an existing **Cisco VPN** template. The **Cisco VPN** template corresponds to the service-side VPN you want to configure NAT for.

Configure a Dynamic NAT Pool

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

2. Click **Feature Templates**.



Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. To edit a **Cisco VPN** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Under **NAT Pool**, click **New NAT Pool**.
6. Enter the required parameters and click **Update**.

Table 3: NAT Pool Parameters

Parameter Name	Description
NAT Pool Name	Enter a NAT pool number configured in the centralized data policy. The NAT pool name must be unique across VPNs and VRFs. You can configure up to 31 (1–31) NAT pools per router.
NAT Pool Prefix Length	Enter the NAT pool prefix length.
NAT Pool Range Start	Enter a starting IP address for the NAT pool. **a.** Change the scope from **Default** to **Global** to enable the field. **b.** Enter the last IP address for the NAT pool.
NAT Pool Range End	Enter a closing IP address for the NAT pool. **a.** Change the scope from **Default** to **Global** to enable the field. **b.** Enter the last IP address for the NAT pool.
NAT Overload	Click **On** to enable per-port translation. Default is **On**. If **NAT Overload** is set to **Off**, only dynamic NAT is configured on the end device. Per-port NAT is not configured.
NAT Direction	Choose the NAT direction.

Configure Service-Side Static NAT

Before You Begin

1. Configure and apply a data policy.

2. Configure a **Cisco VPN** template or edit an existing **Cisco VPN** template.
3. Configure dynamic NAT.

Configure Service-Side Static NAT

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.



Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. To edit a **Cisco VPN** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Click **Static NAT**.
6. Under **Static NAT**, click **New Static NAT**.
7. Enter the required parameters and click **Update**.

Table 4: Static NAT Parameters

Parameter Name	Description
NAT Pool Name	Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can use a NAT pool for static NAT as well. Choose the NAT pool number using the **Global** settings option.
Source IP Address	Enter the inside local address as the source IP address.
Translated Source IP Address	Enter the inside global address as the translated source IP address. Maps a public IP address to a private source address. In Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, if using a NAT pool for static NAT, static translated source IP addresses must be within the configured dynamic NAT pool IP address range.
Static NAT Direction	Select the direction in which to perform network address translation.
Inside	Select **Inside** to translate the IP address of packets that are coming from the service-side of the device and are destined for the transport side of the router.
Outside	Select **Outside** to translate the IP address of packets that are coming to the device from the transport-side device and are destined for a service-side device.

Note In Cisco IOS XE Catalyst SD-WAN Release 17.4.1a and earlier releases up to Cisco IOS XE Catalyst SD-WAN Release 17.3.1a (when the service-side NAT feature was introduced), static NAT IP addresses must not overlap with NAT pool IP addresses.

In Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, static translated source IP addresses may be within the configured dynamic NAT pool IP address range.

Configure Service-Side Port Forwarding for NAT

You can configure port forwarding rules to allow requests from an external network to reach devices on the internal network.

Before You Begin

1. Configure and apply a data policy.
2. Configure a **Cisco VPN** template or edit an existing **Cisco VPN** template.
3. Configure a NAT pool.

Configure Service-Side Port Forwarding for NAT

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. To edit a **Cisco VPN** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Under **NAT Pool**, click **New NAT Pool**.
6. Enter the required NAT pool parameters.

   For more information on the NAT pool parameters, see Configure a NAT Pool and a Loopback Interface.
7. Click **Add**.
8. To create a port forwarding rule, click **Port Forward** > **Add New Port Forwarding Rule** and configure the required parameters.

   You can define up to 128 port-forwarding rules to allow requests from an external network to reach devices on the internal network.

Table 5: Port-Forwarding Parameters

Parameter Name	Description
NAT Pool Name	Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can use a NAT pool for static NAT. Choose the NAT pool number using the **Global** settings option.
Source Port	Enter a port number to define the source port to be translated.*Range:* 0 through 65535
Source IP Address	Enter the source IP address to be translated.
Translate Port	Enter the port number to apply port forwarding to. *Range:* 0 through 65535 In Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, static translated source IP addresses must be within the configured dynamic NAT pool IP address range.
Protocol	Choose the **TCP** or **UDP** protocol to which to apply the port-forwarding rule. To match the same ports for both TCP and UDP traffic, configure two rules.
Translated Source IP Address	Specify the NAT IP address that will be advertised into OMP. Port forwarding is applied to traffic that is destined to this IP address from the overlay with the translated port match.

9. Click **Update**.

Configure Service-Side NAT Using the CLI

Configure a Centralized Data Policy: Match Condition for Source to Any Destination

Configure a centralized data policy that includes a match condition for a source IP to any destination IP.

```
policy
 data-policy edge1
  vpn-list vpn_1
   sequence 101
    match
     source-ip 192.168.11.0/24
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   !
   default-action accept
  !
  vpn-list vpn_2
   sequence 102
    match
     source-ip 192.168.22.0/24
    !
```

```
    action accept
     count nat_vrf_2
     nat pool 2
    !
   !
   default-action accept
  !
  vpn-list vpn_3
   sequence 103
    match
     source-ip 192.168.13.0/24
    !
    action accept
     count nat_vrf_3
     nat pool 3
    !
   !
   default-action accept
  !
 !
 lists
  vpn-list vpn_1
   vpn 1
  !
  vpn-list vpn_2
   vpn 2
  !
  vpn-list vpn_3
   vpn 3
  !
  site-list edge1
   site-id 500
  !
 !
!
```

Configure Inside Dynamic and Static NAT

Configure inside dynamic and static NAT for the NAT pools.

```
ip nat pool natpool1 10.11.11.1 10.11.11.2 prefix-length 24
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload
!
ip nat pool natpool2 10.22.22.1 10.22.22.2 prefix-length 24
ip nat outside source list global-list pool natpool2 vrf 2 overload match-in-vrf
ip nat outside source static 192.168.22.10 10.22.22.10 vrf 2 match-in-vrf
!
ip nat pool natpool3 10.13.13.1 10.13.13.2 prefix-length 24
ip nat inside source list global-list pool natpool3 vrf 3 match-in-vrf overload
ip nat inside source static tcp 192.168.13.10 80 10.13.13.10 8080 vrf 3 extendable
match-in-vrf
```

Configure Static NAT Using NAT Pool for Inside Static NAT (Starting Cisco IOS XE Catalyst SD-WAN Release 17.5.1a)

Configure static NAT inside for a NAT pool.

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
```

Configure static NAT inside and static NAT outside for a NAT pool.

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
ip nat outside source static 192.168.21.10 10.22.22.10 vrf 1 match-in-vrf pool natpool1
```

Use Case 1: Inside Static NAT Using an Inside NAT Pool

In this example, when only the static inside NAT is mapped to the NAT pool, sequence 101 specifies the data-policy configuration for static NAT traffic destined to the service-side of the network from the remote edge through the overlay network (in to out). Sequence 102 specifies the data-policy configuration for traffic from service-side of the network destined to the remote edge device for a destination global IP address of 10.11.11.10 (out to in).

```
policy
 data-policy edge1
  vpn-list vpn_1
   sequence 101
    match
     source-ip 192.168.11.0/24
     destination-ip 192.168.21.0/24
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   !
   default-action accept
  !
 sequence 102
    match
     source-ip 192.168.21.0/24
     destination-ip 10.11.11.0/27
    !
    action accept
     count nat_vrf_2
     nat pool 2
    !
   !
   default-action accept
  !
   default-action accept
  !
 !
```

Use Case 2: Static Inside NAT and Static Outside NAT Mapped to Inside NAT Address Pool

In this example, when the static inside NAT and static outside NAT are mapped to the NAT pool, sequence 101 specifies the data-policy configuration for static NAT traffic destined to the service-side of the network from the remote edge devices through the overlay network (in to out). Sequence 102 specifies the data-policy configuration for traffic from service-side of the network destined to the remote edge device for a destination global IP address of 10.11.11.10 (out to in).

```
policy
data-policy vedge1
  vpn-list vpn_1
   sequence 101
    match
     source-ip 192.168.11.0/24
```

```
     destination-ip 10.22.22.10/27
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   !
   sequence 102
    match
     source-ip 192.168.21.0/24
     destination-ip 10.11.11.0/27
    action accept
     nat pool 1
  default-action accept
 !
```

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, the **ip nat settings central-policy** command is required for NAT on Cisco IOS XE Catalyst SD-WAN devices to work in Cisco Catalyst SD-WAN mode. If you use a Cisco SD-WAN Manager feature template to enable NAT on the device, Cisco SD-WAN Manager automatically pushes this command to the device. However, if you are using a device CLI template only to configure NAT on the device, you need to add the **ip nat settings central-policy** command to the device CLI template configuration.

Verify Configuration of Service-Side NAT

Example for VRF 1

Traffic from 192.168.11.10 gets translated based on the static NAT rule. Traffic from any other source in 192.168.11.0/24 gets translated to a pool IP.

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.13.13.10:8080      192.168.13.10:80      ---                   ---
---  ---                   ---                   10.22.22.10           192.168.22.10

---  10.11.11.10           192.168.11.10         ---                   ---
icmp 10.11.11.1:18193      192.168.11.2:18193    192.168.21.2:18193    192.168.21.2:18193
tcp  10.11.11.10:59888     192.168.11.10:59888   192.168.21.10:21      192.168.21.10:21
tcp  10.11.11.10:50069     192.168.11.10:50069   192.168.21.10:35890   192.168.21.10:35890
tcp  10.11.11.10:39164     192.168.11.10:39164   192.168.21.10:80      192.168.21.10:80
Total number of translations: 7
```

Example for VRF 2

Traffic from 192.168.22.10 gets translated to 10.22.22.10 based on the static NAT rule. Traffic from any other source 192.168.22.0/24 gets translated to a pool IP.

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.13.13.10:8080      192.168.13.10:80      ---                   ---
---  ---                   ---                   10.22.22.10           192.168.22.10

---  10.11.11.10           192.168.11.10         ---                   ---
tcp  192.168.12.10:21      192.168.12.10:21      10.22.22.10:56602     192.168.22.10:56602
tcp  192.168.12.10:46238   192.168.12.10:46238   10.22.22.10:49532     192.168.22.10:49532
icmp 10.22.22.1:18328      192.168.22.2:18328    192.168.12.2:18328    192.168.12.2:18328
```

```
tcp  192.168.12.10:80      192.168.12.10:80      10.22.22.10:46340     192.168.22.10:46340
Total number of translations: 7
```

Example for VRF 3

Any traffic to 10.13.13.10:8080 gets translated to 192.168.13.10:80. Any other traffic from 192.168.11.0/24 gets translated to a pool IP.

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.13.13.10:8080      192.168.13.10:80      ---                   ---
---  ---                   ---                   10.22.22.10           192.168.22.10

---  10.11.11.10           192.168.11.10         ---                   ---
tcp  10.13.13.1:43162      192.168.13.10:43162   192.168.23.10:21      192.168.23.10:21
tcp  10.13.13.1:41753      192.168.13.10:41753   192.168.23.10:34754   192.168.23.10:34754
icmp 10.13.13.1:19217      192.168.13.2:19217    192.168.23.2:19217    192.168.23.2:19217
tcp  10.13.13.10:8080      192.168.13.10:80      192.168.23.10:40298   192.168.23.10:40298
tcp  10.13.13.1:43857      192.168.13.10:43857   192.168.23.10:80      192.168.23.10:80
Total number of translations: 8
```

Verify Service-Side NAT when a NAT Pool is Used for Static NAT (From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a)

The following sample output shows UDP traffic from client 1 (192.168.11.10) to server 2 (192.168.21.11):

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.2            192.168.11.10         ---                   ---
---  10.11.11.5            192.168.11.10         ---                   ---
udp  10.11.11.5:5001       192.168.11.10:5001    192.168.21.11:5001    192.168.21.11:5001
----> NAT IP from Pool 2
Total number of translations: 3
```

The following sample output shows UDP traffic from client 1 (192.168.11.10) to server 1 (192.168.21.10):

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.2            192.168.11.10         ---                   ---
---  10.11.11.5            192.168.11.10         ---                   ---
udp  10.11.11.5:5001       192.168.11.10:5001    192.168.21.11:5001    192.168.21.11:5001
----> NAT IP from Pool 2
udp  10.11.11.2:5001       192.168.11.10:5001    192.168.21.10:5001    192.168.21.10:5001
----> NAT IP as per static NAT rule mapped to Pool 1
Total number of translations: 4
```

The following sample output shows UDP traffic from client 2 (192.168.11.11) to server 2 (192.168.21.11):

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.2            192.168.11.10         ---                   ---
---  10.11.11.6            192.168.11.11         ---                   ---
---  10.11.11.5            192.168.11.10         ---                   ---
udp  10.11.11.5:5001       192.168.11.10:5001    192.168.21.11:5001    192.168.21.11:5001
----> NAT IP from pool 2
udp  10.11.11.6:5001       192.168.11.11:5001    192.168.21.11:5001    192.168.21.11:5001
----> NAT IP from pool 2
udp  10.11.11.2:5001       192.168.11.10:5001    192.168.21.10:5001    192.168.21.10:5001
----> NAT IP as per static NAT rule mapped to Pool 1
Total number of translations: 6
```

Configuration Examples for Service-Side NAT

Example: NAT Configuration on a Cisco VPN Interface Ethernet Template

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
  ip nat translation tcp-timeout 3600
  ip nat translation udp-timeout 60
  ip nat route vrf 1 10.0.0.1 10.0.0.1 global

interface GigabitEthernet1
   no shutdown
   arp timeout 1200
   ip address 10.1.15.15 255.255.255.0
   ip redirects
   ip mtu    1500
   ip nat outside
```

Example: Configuration of Dynamic NAT

```
ip nat pool natpool-gigabitethernet1-0 198.51.100.1 198.51.100.2 prefix-length 24
ip nat inside source list global-list pool natpool-gigabitethernet1-0 egress-interface
GigabitEthernet1
```

Example: Configuration of Interface Overload

```
ip nat pool natpool-gigabitethernet1-0 209.165.201.1 209.165.201.2 prefix-length 24
ip nat inside source list global-list pool natpool-gigabitethernet1-0 overload
egress-interface GigabitEthernet1
```

Example: Configuration of Interface Overload with a Loopback Interface

```
ip nat inside source list global-list interface loopback1 overload egress-interface
GigabitEthernet1
```

Intra-VPN Service-Side NAT

The following sections provide information about configuring intra-VPN service-side NAT.

Information About Intra-VPN Service-Side NAT

Intra-VPN service-side NAT is an extension to service-side NAT, which allows a service-side LAN interface to communicate with another service-side LAN interface within the same VPN. Intra-VPN service-side NAT uses static or dynamic NAT so that data traffic can be initiated in either direction. You can apply static or dynamic NAT rules for packets to be routed from other LAN interfaces to the interface configured as the outside interface using the **ip nat outside** command.

You configure intra-VPN service-side NAT using a device CLI template or a CLI add-on template.

You can configure port forwarding for intra-VPN service-side NAT.

For more information on configuring port forwarding for intra-VPN service-side NAT, see Configure Service-Side Port Forwarding for NAT.

Benefits of Intra-VPN Service-Side NAT

- Supports LAN-to-LAN traffic in the same VPN
- Supports static or dynamic NAT for a mapping between real and mapped IP addresses
- Supports bidirectional traffic between two LAN interfaces within the same VPN

Restrictions for Intra-VPN Service-Side NAT

- NAT for a service-side LAN interface to a remote branch is not supported.
- Direct Internet Access (DIA) is not supported for packets from a service-side LAN interface.
- A service-to-service-side LAN interface must be in the same VPN.

  NAT is not supported across different VPNs.
- Firewall, AppNav-XE, and multicast are not supported.
- Configure intra-VPN service-side NAT using a device CLI template or a CLI add-on template. Cisco SD-WAN Manager feature template support is not available for Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

Note If you use a Cisco SD-WAN Manager feature template for other NAT-related features, **ip nat outside** configuration is removed from the interface. Consequently, intra-VPN service-side NAT functionality is not available.

- Configure the data policy direction as **All** (all directions).
- Only LAN-side physical interfaces and Ethernet sub interfaces are supported. Loopback and Bridge Domain Interface (BDI) interfaces are not supported.
- NAT DIA with port forwarding is not supported.

Configure Intra-VPN Service-Side NAT

Workflow for Configuring Intra-VPN Service-Side NAT

1. Configure a centralized data policy for the Cisco Catalyst SD-WAN Controller for static or dynamic NAT mapping.

   For more information on configuring a centralized data policy, see Create and Apply a Centralized Data Policy for NAT.
2. Configure static or dynamic NAT using a **Cisco VPN** template.
3. (Optional) Configure a pool name for static or dynamic NAT mapping.

   For more information on configuring a pool name for static or dynamic NAT mapping, see Configure Service-Side Static NAT.

4. Use a device CLI template or a CLI add-on template to configure an outside interface for NAT translation and apply the configurations to the device.
5. Attach the device CLI template or the CLI add-on template to the device.

Configure Intra-VPN Service-Side NAT Using a CLI Add-On Template

Before You Begin

Create a new CLI add-on template or edit an existing CLI add-on template.

For more information on CLI add-on feature templates, see CLI Add-On Feature Templates.

Configure Intra-VPN Service-Side NAT Using a CLI Add-On Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose a device from the device list.
5. Click **CLI Add-On Template** under **OTHER TEMPLATES**.
6. In **CLI Add-On Template** area, enter the configuration.
7. Configure an outside interface using the **ip nat outside** command.
8. Click **Save**.

   The CLI add-on template that you created is displayed in the **CLI Configuration** table.
9. Attach the CLI add-on template to your device.

Configuration Examples for Intra-VPN Service-Side NAT

Example: Policy Configuration

The following is a sample configuration of a centralized data policy for the Cisco Catalyst SD-WAN Controller that includes a NAT pool:

```
Device# show running policy
policy
data-policy cedge1
vpn-list vpn_1
sequence 101
match
source-ip 192.168.11.0/24
!
action accept
```

```
count nat_vrf_1
nat pool 1
!
!
default-action accept
!
!
lists
vpn-list vpn_1
vpn 1
!
site-list cedge1
site-id 500
.
.
.
```

Example: LAN Interface 1 Configured with IP NAT Outside

The following example shows that an **ip nat outside** interface has been configured on the GigabitEthernet 5.102 interface.

```
Device# interface GigabitEthernet5.102
encapsulation dot1Q 102
vrf forwarding 1
ip address 192.168.12.1 255.255.255.0
ip mtu 1496
ip nat outside
ip ospf dead-interval 40
ip ospf 1 area 0
pool configuration:
ip nat pool natpool1 10.11.11.1 10.11.11.2 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload

static nat inside config:
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vr
end
```

Example: LAN Interface 2

The following example shows that the GigabitEthernet 5.101 interface has been configured on the same VPN and VRF.

```
Device# interface GigabitEthernet5.101
encapsulation dot1Q 101
vrf forwarding 1
ip address 192.168.11.1 255.255.255.0
ip mtu 1496
ip ospf dead-interval 40
ip ospf 1 area 0
pool configuration:
ip nat pool natpool1 10.11.11.1 10.11.11.2 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload

static nat inside config:
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vr
end
```

Service-Side Conditional Static NAT

The following sections provide information about configuring service-side conditional static NAT.

Information About Service-Side Conditional Static NAT

Configure service-side conditional static NAT to translate the same source IP address to different global IP addresses based on the destination IP addresses.

Service-side conditional static NAT allows you to configure the same source IP address within another configured static NAT pool IP address range. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, this functionality was not supported.

Configure service-side conditional static NAT using a device CLI.

Benefits of Service-Side Conditional Static NAT

- Translates the same source IP address to different IP addresses based on the destination IP addresses in a data policy.
- Allows you to use the same source IP address within another configured static NAT pool IP address range.

Restrictions for Service-Side Conditional Static NAT

- Service-side conditional static NAT is for inside static NAT and service-side traffic only.
- Outside static NAT is not supported.
- DIA traffic is not supported.

Workflow for Configuring Service-Side Conditional Static NAT

1. Configure a centralized data policy and configure the sequences with different destination IP addresses.

   For more information, see Create and Apply a Centralized Data Policy for Service-Side NAT.

2. Configure at least two NAT pools with the same local IP address.

   For more information on configuring service-side conditional static NAT using the CLI, see Configure Service-Side Conditional Static NAT Using the CLI.

3. Verify the translations for the destination IP addresses.

   For more information on verifying the translations for the destination IP addresses, see Verify Conditional Static NAT Using the CLI.

Configure Service-Side Conditional Static NAT Using the CLI

1. Configure a centralized data policy and configure the sequences:

```
data-policy EDGE1
vpn-list vpn_1
sequence 101
match
source-ip 192.168.11.10/32
destination-ip 192.168.21.10/32
!
action accept
count vrf1_In2Out1
nat pool 1
!
!
sequence 102
match
source-ip 192.168.11.10/32
destination-ip 192.168.21.2/32
!
action accept
count vrf1_In2Out2
nat pool 2
!
!
default-action accept
!
!
lists
vpn-list vpn_1
vpn 1
!
site-list EDGE1
site-id 500
!
!
!
```

2. Configure at least two NAT pools:

```
Device(config)# ip nat pool natpool1 10.11.11.1 10.11.11.10 prefix-length 24
Device(config)# ip nat pool natpool2 10.22.22.1 10.22.22.10 prefix-length 24
```

3. Configure inside static NAT using the same source IP address for the corresponding NAT pools:

```
Device(config)# ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf
 pool natpool1
Device(config)# ip nat inside source static 192.168.11.10 10.22.22.10 vrf 1 match-in-vrf
 pool natpool2
Device(config)# ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
overload
Device(config)# ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
overload
```

Verify Service-Side Conditional Static NAT Configuration

Sample Source IP Translations for NAT Pool 1 and NAT Pool 2

For natpool1, the Cisco IOS XE Catalyst SD-WAN device translates the source IP address `192.168.11.10` to `10.11.11.10`, which is destined for `192.168.21.10`.

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.10           192.168.11.10         ---                   ---
---  10.22.22.10           192.168.11.10         ---                   ---
```

```
icmp 10.22.22.10:8371      192.168.11.10:8371    192.168.21.2:8371    192.168.21.2:8371
icmp 10.11.11.10:8368      192.168.11.10:8368    192.168.21.10:8368   192.168.21.10:8368
Total number of translations: 4
```

For natpool2, the Cisco IOS XE Catalyst SD-WAN device translates the source IP address `192.168.11.10` to `10.22.22.10`, which is destined for `192.168.21.2`.

Service-Side Static Network NAT

The following sections provide information about configuring service-side static network NAT.

Information About Service-Side Static Network NAT

You can configure service-side static NAT for an entire network using one configuration.

You can configure service-side static network NAT using Cisco SD-WAN Manager or a device CLI template.

Benefits of Service-Side Static Network NAT

- Supports configuration of a single static NAT pool for configuring an entire subnet.
- Supports the object tracker functionality for LAN prefixes and LAN interfaces.

Restrictions for Service-Side Static Network NAT

- Configuration of service-side static network CLI using a centralized data policy is not supported. But needs a data policy for the CLI to work.
- Overlapping of NAT pool addresses is not supported.
- Only inside service-side network NAT is supported.
- Outside static network NAT is not supported.
- DIA configuration is not supported.

Configure Service-Side Static Network NAT

Before You Begin

- Configure and apply a data policy.

  For more information on creating and applying a centralized data policy for service-side NAT, see Create and Apply a Centralized Data Policy for Service-Side NAT.

- Configure a **Cisco VPN** template or edit an existing **Cisco VPN** template.
- Configure service-side static NAT.

Note You need to configure a NAT pool prior to configuring service-side static network NAT.

For more information on configuring service-side static NAT and a NAT pool, see Configure Service-Side Static NAT.

Configure Service-Side Static Network NAT

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. To edit a **Cisco VPN** template, click **…** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Click **Static NAT**.
6. Under **Static NAT**, click **New Static NAT Subnet**.
7. Enter the required parameters.

Table 6: New Static NAT Subnet Parameters

Parameter Name	Description
Source IP Subnet	Enter the inside local address as the source IP subnet address.
Translated Source IP Subnet	Enter the outside global subnet address as the translated source IP subnet address. Maps a public IP address to a private source address.
Network Prefix Length	Enter the network prefix length.
Static NAT Direction	Select the direction for the network address translation. Choose **Inside** as the direction for performing network address translation.
Add Object /Group Tracker	(Optional) Enter the object ID number if you want to track an object. The object tracker functionality is supported for service-side static network NAT.

8. Click **Update**.

Configure Service-Side Static Network NAT Using the CLI

1. Configure service-side static network NAT using the following command:

```
Device(config)# ip nat inside source static network 192.168.11.0 192.168.70.0 /24 vrf 1
match-in-vrf
```

2. (Optional) Configure a service-side NAT object tracker.

For more information, see Configure Service-Side NAT Object Tracker.

Verify Service-Side Static Network NAT Configuration

The following sections provide information on how to verify service-side static network NAT configuration.

Verify Translations for Service-Side Static Network NAT

The following is a sample output from the **show ip nat translations** command:

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  192.168.70.0          192.168.11.0          ---                   ---
---  192.168.70.11         192.168.11.11         ---                   ---
---  192.168.70.10         192.168.11.10         ---                   ---
icmp 192.168.70.11:16528   192.168.11.11:16528   192.168.21.11:16528   192.168.21.11:16528
icmp 192.168.70.10:16525   192.168.11.10:16525   192.168.21.10:16525   192.168.21.10:16525
icmp 192.168.70.10:16526   192.168.11.10:16526   192.168.21.10:16526   192.168.21.10:16526
icmp 192.168.70.10:16527   192.168.11.10:16527   192.168.21.10:16527   192.168.21.10:16527
```

Verify Service-Side Static Network NAT Route Creation

The following is a sample output from the **show ip route vrf** command:

```
Device# show ip route vrf 1
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
n Nd     10.0.1.0/24 [6/0], 2d00h, Null0
C        10.0.100.0/24 is directly connected, GigabitEthernet8
L        10.0.100.15/32 is directly connected, GigabitEthernet8
C        10.20.24.0/24 is directly connected, GigabitEthernet5
L        10.20.24.15/32 is directly connected, GigabitEthernet5
n Ni  192.168.70.0/24 [7/0], 00:00:12, Null0
```

Application-Level Gateways with Service-Side NAT

The following sections provide information about configuring application-level gateways (ALGs) with Service-Side NAT.

Information About Using ALGs with Service-Side NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, Cisco Catalyst SD-WAN Manager Release 20.15.1

An application-level gateway (ALG), also known as an application-layer gateway, is an application that translates the IP address inside the payload of an application packet. Use an ALG to interpret the application-layer protocol and perform firewall and NAT translations.

Specific protocols that embed the IP address information within the packet payload require the support of an ALG. The following protocol requires an ALG for NAT translations of the application payload:

- File Transfer Protocol (FTP)

For more information about ALGs, see the *IP Addressing: NAT Configuration Guide*.

Benefits of Using ALGs with Service-Side NAT

- Allows client applications to use dynamic TCP or UDP ports to communicate with the server application.

Restrictions for Using ALGs with Service-Side NAT

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, Cisco Catalyst SD-WAN Manager Release 20.15.1

- Outside NAT:
  - You cannot configure ALGs with Service-Side NAT using the **ip nat outside source** command.

Configure ALGs with Service-Side NAT Using a CLI Template

For more information on using CLI templates, see CLI Templates and CLI Add-On Feature Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure ALGs with service-side NAT:

1. Configure service-side NAT.

   For more information, see Configure Service-Side NAT.

2. Enable NAT ALG global support.

   ```
   ip nat service all-algs
   ```

3. Enable NAT ALG for FTP as shown in the following example:

   ```
   ip nat service ftp
   ```

4. Configure NAT pool on the router

```
ip nat pool pool-name pool-range prefix/length
ip nat inside  source list global-list pool pool-name vrf number match-in-vrf
overload
```

Here's the complete configuration example for configuring ALGs.

Configure a centralized data policy that includes a match condition for a source IP to any destination IP

```
policy
 data-policy vedge1
  vpn-list vpn_1
   sequence 101
    match
     destination-ip 203.0.113.21/32
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   sequence 102
    match
     source-ip 198.51.100.150/32
    !
    action accept
     count nat_vrf_1
     nat pool 1
   !
   default-action accept
  !
 !
 lists
  vpn-list vpn_1
   vpn 1
  !
  site-list vedge1
   site-id 500
  !
 !
!
apply-policy
 site-list vedge1
  data-policy vedge1 all
```

Enable NAT ALG global support

```
ip nat service all-algs
```

Enable NAT ALG for FTP

```
ip nat service ftp
```

Configure NAT pool on the router

```
ip nat pool natpool1 203.0.113.21 203.0.113.21 prefix-length 24
ip nat inside source static 192.0.2.150 203.0.113.99 vrf 1 match-in-vrf pool natpool1
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload
```

Verify ALG Configuration

The following sections provide information about verifying configuration of ALG with service-side NAT.

Display NAT Translations

```
show ip nat translations tcp
tcp  203.0.113.21:37713     192.0.2.150:37713    198.51.100.150:21       198.51.100.150:21
tcp  203.0.113.21:40586     192.0.2.150:40586    198.51.100.150:38366    198.51.100.150:38366
```

Note You cannot view the translation of the payload using a CLI template. To view the translation of a payload, capture a packet using Cisco SD-WAN Manager.

For more information on capturing packets using Cisco SD-WAN Manager, see Capture Packets in the *Cisco Catalyst SD-WAN Monitor and Maintain Guide*.

Display ALG Translations

```
Device(config)# show platform hardware qfp active feature nat datapath sess-dump

id 0xeec305c0 io 192.0.2.150 oo 198.51.100.150 io 51967 oo 27734 it 203.0.113.21 ot
198.51.100.150 it 51967 ot 27734 pro 6 vrf 5 tableid 5 bck 8490 in_if 0 out_if 0 ref 1 flags
 0xc0204014 ext_flags 0x0 in_pkts 783 in_bytes 1073640 out_pkts 435 out_bytes 13928 flowdb
 in2out fh 0x0 flowdb out2in fh 0x0 rg 0
id 0xeec30470 io 192.0.2.150 oo 198.51.100.150 io 37715 oo 21 it 203.0.113.21 ot
198.51.100.150 it 37715 ot 21 pro 6 vrf 5 tableid 5 bck 12489 in_if 0 out_if 0 ref 1 flags
 0xc0204014 ext_flags 0x0 in_pkts 15 in_bytes 597 out_pkts 16 out_bytes 788 flowdb in2out
fh 0x0 flowdb out2in fh 0x0 rg 0
```

Display NAT Statistics

```
Device(config)# show platform hardware qfp active feature nat datapath stats

Counter                                                          Value
------------------------------------------------------------------------
number_of_session                                                    2
udp                                                                  0
tcp                                                                  2
icmp                                                                 0
non_extended                                                         1
statics                                                              1
static_net                                                           0
entry_timeouts                                                       0
hits                                                                 0
misses                                                               0
cgn_dest_log_timeouts                                                0
ipv4_nat_alg_bind_pkts                                               5
ipv4_nat_alg_sd_not_found                                            0
ipv4_nat_alg_sd_tail_not_found                                       0
ipv4_nat_rx_pkt                                                  21686
ipv4_nat_tx_pkt                                                  21892
ipv4_nat_flowdb_hits                                                 0
ipv4_nat_stick_rx_pkts                                               0
ipv4_nat_stick_i2o_pkts                                              0
ipv4_nat_stick_o2i_pkts                                              0
ipv4_nat_stick_forus_hits_pkts                                       0
ipv4_nat_stick_hit_sb                                                0
```

```
ipv4_nat_stick_ha_divert_pkts                                0
ipv4_nat_stick_ha_ar_pkts                                    0
ipv4_nat_stick_ha_tcp_fin                                    0
ipv4_nat_stick_ha_failed_pkts                                0
ipv4_nat_non_natted_in2out_pkts                           2762
ipv4_nat_non_nated_out2in_pkts                           18955
ipv4_nat_bypass_pkts                                         0
ipv4_nat_unmarked_pkts                                   16330
ipv4_nat_res_port_in2out_pkts                                0
ipv4_nat_res_port_out2in_pkts                                0
ipv4_nat_ipc_retry_fail                                      0
ipv4_nat_cfg_rcvd                                            9
ipv4_nat_cfg_rsp                                            13
```