Using a vEdge Router as a NAT Device

A vEdge can act as a NAT device, both on the transport side of the router and on the service side. On the transport side, the NAT functionality allows traffic from a local site to flow directly to the Internet rather than being backhauled to a colo facility that provides NAT services for Internet access. The NAT function is performed as the traffic enters the overlay tunnel to the WAN transport. On the service side, NAT functionality allows traffic from the local site to traverse the NAT before entering the overlay tunnel.

Using a vEdge as a NAT Device on the Transport Side

To provide users at a local site with direct, secure access to Internet resources, such as websites, you can configure the vEdge to function as a Network Address Translation (NAT) device, performing both address and port translation (NAPT). Enabling NAT allows traffic exiting from a vEdge to pass directly to the Internet rather than being backhauled to a colocation facility that provides NAT services for Internet access. Using NAT in this way on a vEdge can eliminate traffic "tromboning" and allows for efficient routes, that have shorter distances, between users at the local site and the network-based applications that they use.

The figure below shows the router acting as a NAT device. The vEdge splits its traffic into two flows, which you can think of as two separate tunnels. One traffic flow, shown in green, remains within the overlay network and travels between the two routers in the usual fashion, on the secure IPsec tunnels that form the overlay network. The second traffic stream, shown in grey, is redirected through the vEdge's NAT device and then out of the overlay network to a public network.

The NAT functionality on a vEdges operates in a standard end-point independent fashion. The NAT software performs both address and port translation (NAPT). It establishes a translation entry between a private address and port pair inside the overlay network and a public address and port outside the overlay network. Once this translation entry is created, the NAT software allows incoming connections from an external host to be established with that private address and port only if that private address and port already established a connection to the external host. That is, an
external host can reply to traffic from the private address and port; it cannot initiate a connection.

The Cisco SD-WAN NAT software supports 64,000 NAT flows.

vEdge provides Application Layer Gateway (ALG) FTP support with Network Address Translation – Direct Internet Access (NAT-DIA), Service NAT, and Enterprise Firewall.

---

### Transport-Side NAT Operation

We use the following figure to explain how the NAT functionality on the vEdge splits traffic into two flows (or two tunnels) so that some of it remains within the overlay network and some goes directly to the Internet or other public network.

In this figure, the vEdge has two interfaces:

- Interface ge0/1 faces the local site and is in VPN 1. Its IP address is 10.1.12.0/24.
- Interface ge0/0 faces the transport cloud and is in VPN 0 (the transport VPN). Its IP address is 192.23.100.0/24, and it uses the default OMP port number, 12346, for overlay network tunnels.

To configure the vEdge to act as a NAT device so that some traffic from the router can go directly to a public network, you do three things:

- Enable NAT in the transport VPN (VPN 0) on the WAN-transport–facing interface, which here is ge0/0. All traffic exiting from the vEdge, going either to other overlay network sites or to a public network, passes through this interface.
- To direct data traffic from other VPNs to exit from the vEdge directly to a public network, enable NAT in those VPNs or...
ensure that those VPNs have a route to VPN 0.

- On the vSmart controller, create a centralized data policy that redirects the desired data traffic from the non-transport VPN to VPN 0, and then apply that data policy to the non-transport VPN. In this case, we apply the policy to VPN 1.

Once NAT is enabled on the vEdge, data traffic affected by the centralized data policy (here, the data traffic from VPN 1) is split into two flows:

- Traffic destined for another vEdge in the overlay network remains in VPN 1, and it travels directly through the IPsec data plane tunnel from the source vEdge to the destination vEdge. This traffic never passes through VPN 0, and therefore it is never touched by NAT.

- Traffic destined for the public network passes from VPN 1 to VPN 0, where it is NATed. During the NAT processing, the source IP address is changed from 10.1.12.0/24 to that of ge0/0, 179.23.100.0/24, and the source port is changed to 1024.

When NAT is enabled, all traffic that passes through VPN 0 is NATed. This includes both the data traffic from VPN 1 that is destined for a public network, and all control traffic, including the traffic required to establish and maintain DTLS control plane tunnels between the vEdge and the vSmart controller and between the router and the vBond orchestrator. The vBond orchestrator learns both the public and private addresses of the vEdge, and it advertises both address to the vSmart controller. In turn, the vSmart controller advertises both addresses to all the vEdges in its domain. Each vEdge then decides whether to use the public or the private address to communicate with another vEdge as follows:

- If the vEdge is located at the same site as the other router (that is, if they are both configured with the same overlay network site ID), it communicates using the private address. Because both routers have the same site ID, they are behind the same NAT, and so their communication channels are already secure.

- If the vEdge route is at a different site, it communicates with the other router using the public address. Then, the NAT functionality on the vEdge translates the public address to the proper private address.

If a vSmart controller connected to a corporate NAT and a NAT-enabled vEdge are located at the same physical overlay network site, you must configure them with different Cisco SD-WAN site identifiers in order for them to be able to communicate. Similarly, if more than one NAT-enabled vEdge is located at the same physical overlay network site, each one must be configured with a different site identifier.

### Using a vEdge as a Service-Side NAT Device

On a vEdge, you can configure NAT on the service side of the router so that data traffic traverses the NAT before entering the overlay tunnel that is located in the transport VPN. The service-side NAT performs NAT to mask the IP address of data traffic it receives. You can configure both dynamic NAT and 1:1 static NAT on the vEdge.

### Service-Side NAT Operation

We use the following figure to explain how the vEdge provides NAT services on the service side:
In this figure, the vEdge has one NAT interface in VPN 1. This interface pools all service-side traffic destined for the NAT interface. The interface name is natpool2, and its IP address is 192.168.10.1. This IP address is the address each packet's IP address is translated to.

To configure the service-side NAT operation on the vEdge so that traffic traverses the NAT in VPN 1 before being placed on the transport tunnel towards its destination, you do two things:

- Create a NAT pool interface in VPN 1, the service-side VPN. Here, the NAT pool number is 2.

- To direct data traffic from prefixes within VPN 1 to the service-side NAT, create a centralized data policy on the vSmart controller. In the match condition, specify the prefixes to be NATed. In the action condition, set the desired NAT pool, here, natpool 2. Then apply the data policy to the desired site (here, site 500), and apply it to traffic coming from the service side.

When service-side NAT is enabled, all matching prefixes in VPN 1 are directed to the natpool2 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, here the data center.

Additional Information

Configuring Local Internet Exit
Configuring NAT Port Forwarding
Configuring Service-Side NAT