Centralized Control Policy Configuration Examples

This article provides some straightforward examples of configuring centralized control policy to help you understand the configuration procedure and get an idea of how to use policy to influence traffic flow across the Viptela overlay network domain. You can find more complex examples in the Validated Examples articles.

Traffic Engineering

This example of traffic engineering forces all traffic to come to a vEdge router via a vEdge hub instead of directly.

One common way to design a domain in a Viptela overlay network is to route all traffic destined for branches through a vEdge hub router, which is typically located in a data center, rather than sending the traffic directly from one vEdge router to another. You can think of this as a hub-and-spoke design, where one vEdge router is acting as a hub and the vEdge routers are the spokes. With such a design, traffic between local branches travels over the IPsec connections that are established between the vEdge spoke routers and the vEdge hub routers when the vEdge routers booted up. Using established connections means that the vEdge routers do not need to expend time and CPU cycles to establish IPsec connections with each other. If you were to imagine that this were a large network with many vEdge routers, having a full mesh of connections between each pair of routers would require a large amount of CPU from the routers. Another attribute of this design is that, from an administrative point of view, it can be simpler to institute coordinated traffic flow policies on the vEdge hub routers, both because there are fewer of them in the overlay network and because they are located in a centralized data center.

One way to direct all vEdge spoke router traffic to a vEdge hub router is to create a policy that changes the TLOC associated with the routes in the local network. Let’s consider the topology in the figure here:
This topology has two vEdge routers in different branches:

- The West vEdge router in site ID 1. The TLOC for this router is defined by its IP address (1.1.1.1), a color (gold), and an encapsulation (here, IPsec). We write the full TLOC address as \(\{1.1.1.1, \text{gold}, \text{ipsec}\}\). The color is simply a way to identify a flow of traffic and to separate it from other flows.

- The East vEdge router in site ID 2 has a TLOC address of \(\{2.1.1.1, \text{gold}, \text{ipsec}\}\).

The West and East vEdge routers learn each other’s TLOC addresses from the OMP routes distributed to them by the vSmart controller. In this example, the East vEdge advertises the prefix 8.8.0.0/16 as being reachable at TLOC \(\{2.1.1.1, \text{gold}, \text{ipsec}\}\). In the absence of any policy, the West vEdge router could route traffic destined for 8.8.0.0/16 to TLOC \(\{2.1.1.1, \text{gold}, \text{ipsec}\}\), which means that the West vEdge router would be sending traffic directly to the East vEdge router.

However, our design requires that all traffic from West to East be routed through the vEdge hub router, whose TLOC address is \(\{100.1.1.1, \text{gold}, \text{ipsec}\}\), before going to the East vEdge router. To effect this traffic flow, you define a policy that changes the route’s TLOC. So, for the prefix 8.8.0.0/16, you create a policy that changes the TLOC associated with the prefix 8.8.0.0/16 from \(\{2.1.1.1, \text{gold}, \text{ipsec}\}\), which is the TLOC address of the East vEdge router, to \(\{10.1.1.1, \text{gold}, \text{ipsec}\}\), which is the TLOC address of the vEdge hub router. The result is that the OMP route for the prefix 8.8.0.0/16 that the vSmart controller advertises to the West vEdge router contains the TLOC address of the vEdge hub router instead of the TLOC address of the East vEdge router. From a traffic flow point of view, the West vEdge router then sends all traffic destined for 8.8.0.0/16 to the vEdge hub router.

The vEdge Hub router also learns the TLOC addresses of the West and East vEdge routers from the OMP routes advertised by the vSmart controller. Because we want vEdge hub router to use these two TLOC addresses, no policy is required to control how the hub directs traffic to the the vEdge routers.

Here is a policy configuration on the vSmart controller that directs the West vEdge router (and any other vEdges in the network domain) to send traffic destined to prefix 8.8.0.0/16 to TLOC 10.1.1.1, gold, which is the vEdge hub router:

```
policy
lists
  prefix-list east-prefixes
  ip-prefix 8.8.0.0/16
  site-list west-sites
  site-id 1
```
control-policy change-tloc
  sequence 10
    match route
      prefix-list east-prefixes
      site-id 2
    action accept
      set tloc 10.1.1.1 color gold encap ipsec
apply-policy
  site west-sites control-policy change-tloc out

A rough English translation of this policy is:

Create a list named "east-prefixes" that contains the IP prefix "8.8.0.0/16"
Create a list named "west-sites" that contains the site-id "1"
Define a control policy named "change-tloc"
Create a policy sequence element that:
  Matches a prefix from list "east-prefixes", that is, matches "8.8.0.0/16"
  AND matches a route from site-id "2"
If a match occurs:
  Accept the route
  AND change the route’s TLOC to "10.1.1.1" with a color of "gold" and an encapsulation of "ipsec"
Apply the control policy "change-tloc" to OMP routes sent by the vSmart controller to "west-sites" and sites in the "west-sites" list.

This control policy is configured on the vSmart controller as an outbound policy, as indicated by the `out` option in the `apply-policy site` command. This option means the the vSmart controller applies the TLOC change to the OMP route after it distributes the route from its route table. The OMP route for prefix 8.8.0.0/16 that the vSmart controller distributes to the West vEdge associates 8.8.0.0/16 with TLOC 10.1.1.1, gold. This is the OMP route that the West vEdge router installs in its route table. The end results are that when the West vEdge router sends traffic to 8.8.0.0/16, the traffic is directed to the vEdge hub; and the West vEdge router does not establish a DTLS tunnel directly with the East vEdge router.

If the West side of the network had many sites instead of just one and each site had its own vEdge router, it would be straightforward to apply this same policy to all the sites. To do this, you simply add the site IDs of all the sites in the `site-list west-sites` list. This is the only change you need to make in the policy to have all the West side sites send traffic bound for the prefix 8.8.0.0/16 through the vEdge hub router. For example:

Creating Arbitrary Topologies

To provide redundancy in the hub-and-spoke-style topology discussed in the previous example, you can add a second vEdge hub to create a dual-homed hub site. The following figure shows that site ID 10 now has two vEdge hubs. We still want all inter-branch traffic to be routed through a vEdge hub. However, because we now have dual-homed hubs, we want to share the data traffic between the two hub routers.
vEdge hub West, with TLOC 10.1.1.1, gold. We want all data traffic from branches on the West side of the overlay network to pass through and be processed by this vEdge router.

vEdge hub East, with TLOC 20.1.1.1, gold. Similarly, we all East side data traffic to pass through the East vEdge hub.

Here is a policy configuration on the vSmart controller that would send West side data traffic through vEdge hub West and East side traffic through vEdge hub East:

```plaintext
policy
lists
  site-list west-sites
  site-id 1
  site-list east-sites
  site-id 2
tloc-list west-hub-tlocs
tloc-id 10.1.1.1 gold
tloc-list east-hub-tlocs
tloc-id 20.1.1.1 gold
control-policy prefer-west-hub
  sequence 10
  match tloc
  tloc-list west-hub-tlocs
  action accept
  set preference 50
control-policy prefer-east-hub
  sequence 10
  match tloc
  tloc-list east-hub-tlocs
  action accept
  set preference 50
apply-policy
  site west-sites control-policy prefer-west-hub out
  site east-sites control-policy prefer-east-hub out
```

Here is an explanation of this policy configuration:
• Create the site lists that are required for the apply-policy configuration command:
  ◦ site-list west-sites lists all the site IDs for all the vEdge routers in the West portion of the overlay network.
  ◦ site-list east-sites lists the site IDs for the vEdge routers in the East portion of the network.

• Create the TLOC lists that are required for the match condition in the control policy:
  ◦ west-hub-tlocs lists the TLOC for the West vEdge hub, which we want to service traffic from the West side vEdge routers.
  ◦ east-hub-tlocs lists the TLOC for the East vEdge hub, to service traffic from the East vEdge routers.

  **Note:** When the control policy is configured to match the TLOC list, the preference option defaults to tloc-list not routes. You can see which option is set using the command `show omp tlocs ip system_IP_address detail`.

• Define two control policies:
  ◦ prefer-west-hub affects OMP routes destined to TLOC 10.1.1.1, gold, which is the TLOC address of the West vEdge hub router. This policy modifies the preference value in the OMP route to a value of 50, which is large enough that it is likely that no other OMP routes will have a larger preference. So setting a high preference value directs traffic destined for site 100 to the West hub router.
  ◦ Similarly, prefer-east-hub sets the preference to 50 for OMP routes destined TLOC 20.1.1.1, gold, which is the TLOC address of the East vEdge hub router, thus directing traffic destined for site 100 site to the East vEdge hub router.

• Apply the control policies:
  ◦ The first line in the apply-policy configuration has the vSmart controller apply the prefer-west-hub control policy to the sites listed in the west-sites list, which here is only site ID 1, so that the preference in their OMP path destined for TLOC 10.1.1.1 is changed to 50 and traffic sent from the West vEdge routers to the hub site goes through the West vEdge hub router.
  ◦ The vSmart controller applies the prefer-east-hub control policy to the OMP paths that it advertises to the vEdges in the east-sites list, which changes the preference to 50 for OMP paths destined for TLOC 20.1.1.1, so that traffic from the East vEdge routers goes to the East vEdge hub router.

---

**Additional Information**

*Configuring Centralized Control Policy*