
Viptela Policy Framework Basics

This article and the next offer an orientation about the architecture of the Viptela policy software used to implement overlay network-wide policies. These policies are called *vSmart policy* or *centralized policy*, because you configure them centrally on a vSmart controller. vSmart policy affects the flow of both control plane traffic (routing updates carried by OMP and used by the vSmart controllers to determine the topology and status of the overlay network) and data plane traffic (data traffic that travels between the vEdge nodes across the overlay network).

With the Viptela software, you can also create vEdge routing policies on the vEdge edge routers. These policies are simply traditional routing policies that are associated with BGP or OSPF locally on the vEdge router. You use them in the traditional sense for controlling BGP and OSPF, for example, to affect the exchange of route information, to set route attributes, and to influence path selection. We do not discuss vEdge routing policy further these two orientation articles.

vSmart Policy Architecture Components

The vSmart policies that implement overlay network-wide policies are implemented on a vSmart controller. Because vSmart controllers are centralized devices, you can manage and maintain vSmart policies centrally, and you can ensure consistency in the enforcement of policy across the overlay network.

The implementation of vSmart policy is done by configuring the entire policy on the vSmart controller. vSmart policy configuration is accomplished with three building blocks:

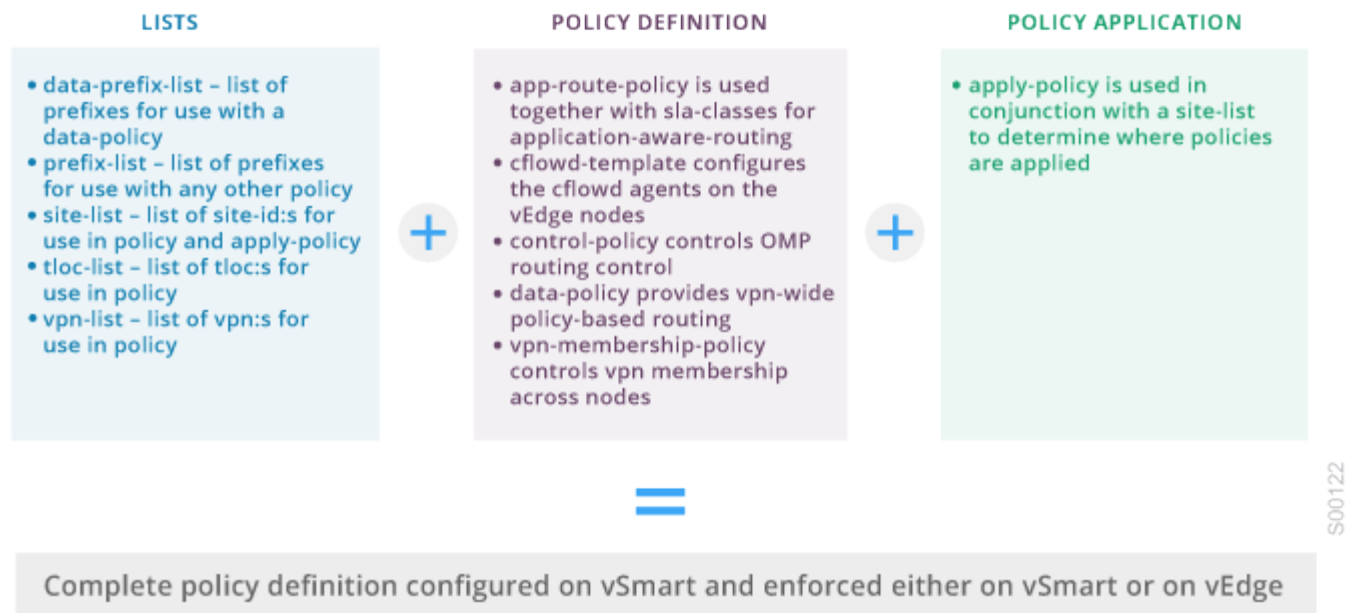
- *Lists* define the targets of policy application or matching.
- *Policy definition*, or *policies*, controls aspects of control and forwarding. There are different types of policy, including:
 - *app-route-policy* (for application-aware routing)
 - *cflowd-template* (for cflowd flow monitoring)
 - *control-policy* (for routing and control plane information)
 - *data-policy* (for data traffic)
 - *vpn-membership-policy* (for limiting the scope of traffic to specific VPNs)
- *Policy application* controls what a policy is applied towards. Policy application is site-oriented, and is defined by a specific list called a site-list.

(In the bulleted list above and throughout this article, we occasionally use the name of the configuration command in text or figures when the meaning is clear. We do this to connect the discussion here with what you see in the software configuration. Configuration commands that are two or more English words use hyphens to separate the words. For example, *app-route-policy* is the command to configure an application-aware routing policy, and the *control-policy* command configures a control policy.)

You assemble these three building blocks to vSmart policy. More specifically, policy is the sum of one or more lists, one



policy definition, and at least one policy applications, as shown in the figure below.



This figure lists the specific configuration keywords used to define lists and policies and to apply the policy. We discuss these in more detail later in this article.

vSmart Policy Operation

Knowing how vSmart policies are constructed, let's look at how they operate. Here, we'll look at the operation of three of the basic vSmart policies: control policy, data policy, and VPN membership policy. We'll example the operation of the other types of vSmart policy later in this article.

At a high level, control policy operates on routing information, which in the Viptela network is carried in OMP updates. Data policy affects data traffic, and VPN membership controls the distribution of VPN routing tables.

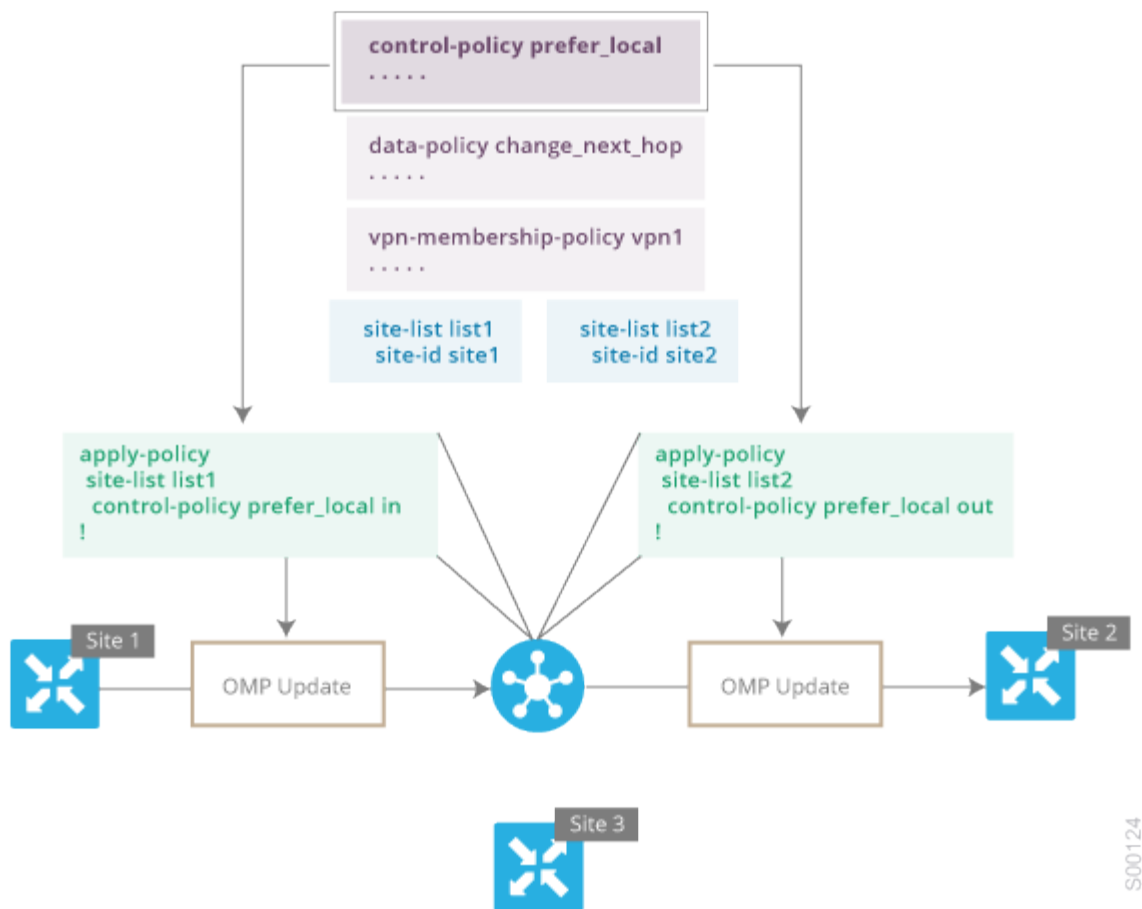
Control Policy Operation

Viptela devices periodically exchange OMP updates, which carry routing information pertaining to the overlay network. Two of the things that these updates contain are vRoute attributes and TLOC attributes. (The specific vRoute and TLOC attributes are discussed later in this article.) The vSmart controller uses these attributes from the OMP updates to determine the topology and status of the overlay network, and installs routing information about the overlay network into its route table. The controller then advertises the overlay topology to the vEdge routers in the network by sending OMP updates to them.

Control policy examines the vRoute and TLOC attributes carried in OMP updates and can modify attributes that match the policy. Any changes that results from control policy are applied directionally, either inbound or outbound (the directionality is from the point of view of the vSmart controller).



The figure below shows a control-policy named "prefer_local" that is configured on a vSmart controller and that is applied to Site 1 (via site-list list1) and to Site 2 (via site-list list2).



The upper left arrow shows the policy being applied to Site 1—more specifically, to **site-list list1**, which contains an entry for Site 1. The command to apply the policy is **control-policy prefer_local in**. The **in** keyword indicates an *inbound* policy: the policy is applied to OMP updates that are coming *in* to the vSmart controller from the vEdge router, which is inbound from the perspective of the controller. So, for all OMP updates that the Site 1 vEdge router sends to the vSmart controller, the "prefer_local" control policy is applied before the updates reach the route table on the vSmart controller. If any vRoute or TLOC attributes in an OMP update match the policy, any changes that result from the policy actions occur before the vSmart controller installs the OMP update information into its route table.

It is important to understand the effect of an inbound policy, because the route table on the vSmart controller is used to determine the topology of the overlay network. The vSmart controller then distributes this topology information, again via OMP updates, to all the vEdge routers in the network. Because applying policy in the inbound direction influences the information available to the vSmart controller to determine the network topology and network reachability, modifying vRoute and TLOC attributes before they are placed in the controller's route table can provide broad influence over the flow of traffic throughout the overlay network.

On the right side of the figure above, we use the same "prefer_local" policy, but here apply it to Site 2 via the **control-**



policy prefer_local out command. The **out** keyword in the command indicates an *outbound policy*, which means that the policy is applied to OMP updates that the vSmart controller is sending to the vEdge router at Site 2. Any changes that result from the policy occur *outbound*, after the information from the vSmart controller's route table has been placed into an OMP update and before the vEdge router receives the update. Again, note that the direction is outbound from the perspective of the vSmart controller.

In contrast to an inbound policy, which affects the centralized route table on the vSmart controller and thus can have a broad effect on the route attributes advertised to all the vEdge routers in the overlay network, a control policy applied in the outbound direction influences only the route tables on the individual vEdge routers included in the site-list, so it generally has a more limited scope.

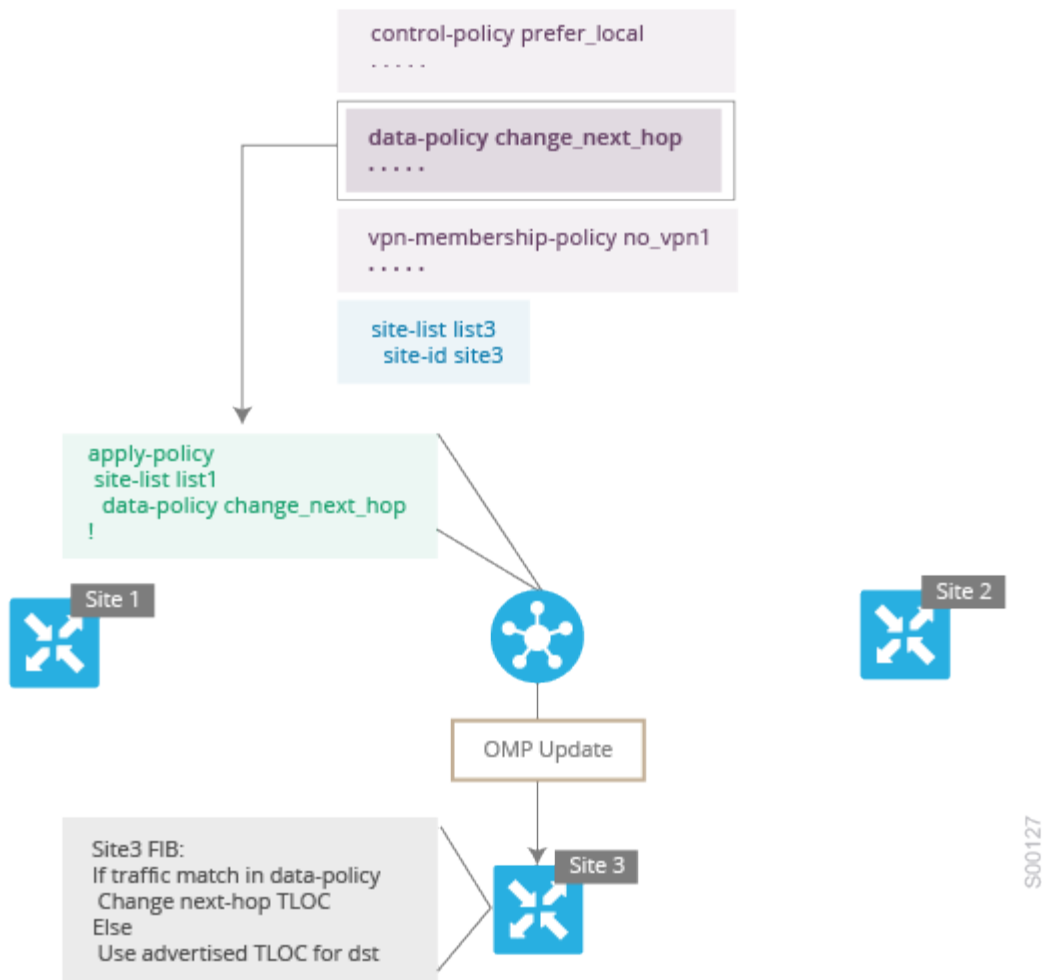
We point out again that in this figure, we are applying the same control policy (the "prefer_local" policy) to both the inbound and outbound OMP updates. However, the affects of applying the same policy inbound and outbound will be different. The usage shown in the figure illustrates the flexibility of the Viptela control policy design architecture and configuration.

Data Policy Operation

Data policy examines fields in the headers of data packets, looking at the source and destination addresses and ports, and the protocol and DSCP values, and for matching packets, it can modify the next hop in a variety of ways or apply a policer to the packets. Data policy is configured and applied on the vSmart controller, and then it is carried in OMP updates to the vEdge routers in the site-list that the policy is applied to. The match operation and any resultant actions are performed on the vEdge router as it transmits or receives data traffic.

In the figure below, a data policy named "change_next_hop" is applied to a list of sites that includes Site 3. The OMP update that the vSmart controller sends to the vEdge router at Site 3 includes this policy definition. When the vEdge router sends or receives data traffic that matches the policy, it changes the next hop to the specified TLOC. Nonmatching traffic is forwarded to the original next-hop TLOC.





In the `apply-policy` command for a data policy, you specify a direction from the perspective of the vEdge router. In the figure, the "all" direction applies the policy to data traffic transiting the tunnel interface, both what the vEdge router is sending and what it is receiving. You can limit the span of the policy to only incoming traffic (with a **`data-policy change_next_hop from-tunnel`** command) or to only outgoing traffic (with a **`data-policy change_next_hop from-service`** command).

VPN Membership Policy Operation

VPN membership policy, as the name implies, affects the VPN route tables that are distributed to particular vEdge routers. In an overlay network with no VPN membership policy, the vSmart controller pushes the routes for all VPNs to all vEdge routers. If your business usage model restricts participation of specific vEdge routers in particular VPNs, a VPN membership policy is used to enforce this restriction.

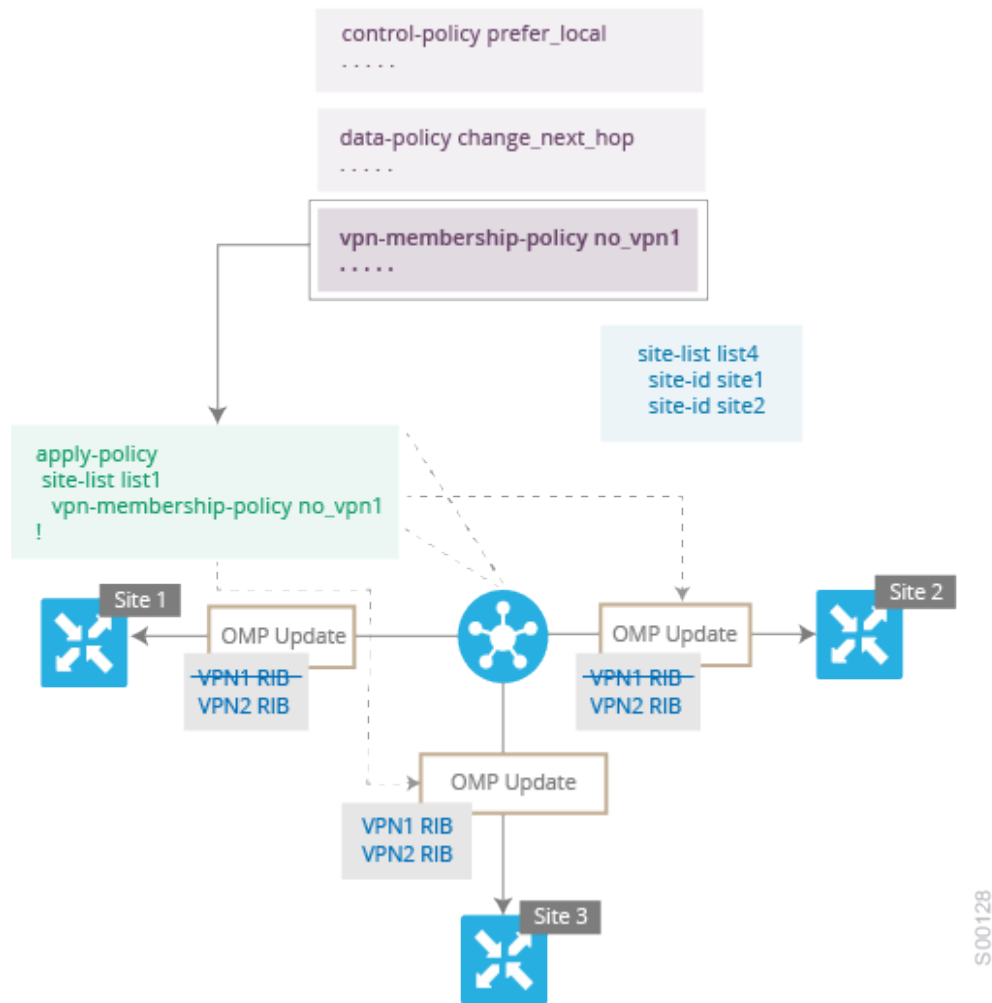
The figure below illustrates how VPN membership policy works. This topology has three vEdge routers:

- The vEdge routers at Sites 1 and 2 service only VPN 2.



- The vEdge router at Site 3 services both VPN 1 and VPN 2.

So here, we want the router at Site 3 to receive all route updates from the vSmart controller, because these updates are for both VPN 1 and VPN 2. However, because the other two routers service only VPN 2, we can filter the route updates sent to them, removing the routes associated with VPN 1 and sending only the ones that apply to VPN 2.




Notice that here, also, you don't set a direction when applying VPN membership policy. This vSmart controller always applies this type of policy to the OMP updates that it sends outwards to the vEdge routers.

Configuring and Executing vSmart Policies

All vSmart policies are configured on the vSmart controller, using a combination of policy definition and lists. All vSmart policies are also applied on the vSmart controller, with a combination of `apply-policy` and lists. However, where the actual vSmart policy executes depends on the type of policy, as shown in this figure:



 vSmart	Action	App-route Policy	Cflowd Template	Control Policy	Data Policy	VPN Membership Policy
	Configure	✓	✓	✓	✓	✓
	Apply	✓	✓	✓	✓	✓
	Execute			✓		✓

 vEdge	Action	App-route Policy	Cflowd Template	Control Policy	Data Policy	VPN Membership Policy
	Configure					
	Apply					
	Execute	✓	✓		✓	

S00141

For control policy and VPN membership policy, the entire policy configuration remains on the vSmart controller, and the actions taken as a result of routes or VPNs that match a policy are performed on the vSmart controller.

For the other three policy types—application-aware routing, cflowd templates, and data policy—the policies themselves are transmitted in OMP updates to the vEdge routers, and any actions taken as a result of the policies are performed on the vEdge routers.

vSmart Policy Components

Now let's discuss the software components used to construct policy in a bit more detail.

Lists

Lists are how you group related items so that you can reference them all together. Examples of items you put in lists are prefixes, TLOCs, VPNs, and overlay network sites. In vSmart policy, you invoke lists in two places: when you create a policy definition and when you apply a policy. Separating the definition of the related items from the definition of policy means that when you can add or remove items from a lists, you make the changes only in a single place: You do not have to make the changes through the policy definition. So if you add ten sites to your network and you want to apply an existing policy to them, you simply add the site identifiers to the site list. You can also change policy rules without having to manually modify the prefixes, VPNs, or other things that the rules apply to.

The illustration below shows the types of vSmart policy lists:



```

policy
lists
data-prefix-list app1
ip-prefix 1.1.1.1/32 port 100
!
prefix-list pfx1
ip-prefix 1.1.1.1/32
!
site-list site1
site-id 100
!
tloc-list site1_tloc
tloc 1.1.1.1 color mpls
vpn-list vpn1
vpn 1
!
!
!

```

S00129

data-prefix-list is used in data-policy to define prefix and upper layer ports, either individually or jointly, for traffic matching.

prefix-list is used in control-policy to define prefixes for matching RIB entries.

site-list is used in control-policy to match source sites, and in apply-policy to define sites for policy application.

tloc-list is used in control-policy to define TLOCs for matching RIB entries and to apply redefined TLOCs to vRoutes.

vpn-list is used in control-policy to define prefixes for matching RIB entries, and in data-policy and app-route-policy to define VPNs for policy application.

Policy Definition

The policy definition is where you create the policy rules. You specify match conditions (route-related properties for control policy and data-related fields for data policy) and actions to perform when a match occurs. A policy contains match–action pairings that are numbered and that are examined in sequential order. When a match occurs, the action is performed, and the policy analysis on that route or packet terminates. Some types of policy definitions apply only to specific VPNs.

The following figure shows the components of the vSmart policy definition. These items are listed in the logical order you should use when designing policy, and this order is also how the items are displayed in the configuration, regardless of the order in which you add them to the configuration.

```

policy
policy-type name
vpn-list vpn-list
sequence number
match
<route | tloc | vpn | other>
!
action <accept | reject | drop>
set attribute value
!
default-action <reject | accept>
!
!
!

```

S00130

policy-type—which can be **control-policy**, **data-policy**, or **vpn-membership** (as well as a few other keywords that we discuss later)—dictates the type of policy. Each type has a particular syntax and a particular set of match conditions and settable actions.

vpn-list is used by data-policy and app-route-policy to list the VPNs for which the policy is applicable.

sequence defines each sequential step of the policy by sequence number.

match decides what entity to match on in the specific policy sequence.

action determines the action that corresponds to the preceding match statement.

default-action is the action to take for any entity that is not matched in any sequence of the policy. By default, the action is set to reject.



Policy Application

For a policy definition to take effect, you associate it with sites in the overlay network.

```
apply-policy
site-list name
control-policy name <in|out>
!
site-list name
data-policy name
vpn-membership name
!
```

S00131

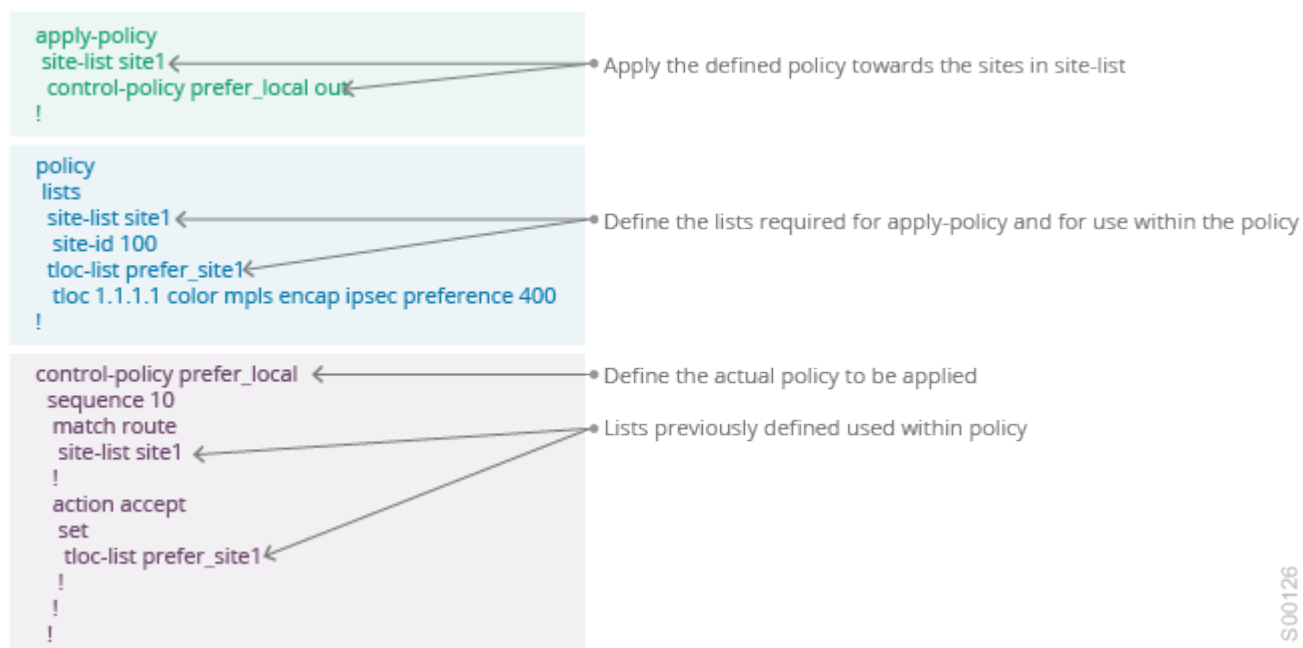
The following are the configuration components:

site-list determines the sites to which a given policy is applied. The direction (in | out) applies only to control-policy.

The policy type—**control-policy**, **data-policy**, **vpn-membership**—and name refer to an already configured policy to be applied to the sites specified in the site-list for the section.

Policy Example

Now, let's put together a complete policy, which consists of lists, policy definition, and policy application. The example illustrated below creates two lists (a site-list and a tloc-list), defines one policy (a control policy), and applies the policy to the site-list. In the figure, the items are listed as they are presented in the node configuration. In a normal configuration process, you create lists first (group together all the things you want to use), then define the policy itself (define what things you want to do), and finally apply the policy (specify the sites that the configured policy affects).



TLOC Attributes Used in Policies

A transport location, or TLOC, defines a specific interface in the overlay network. Each TLOC consists of a set of attributes that are exchanged in OMP updates among the Viptela devices. Each TLOC is uniquely identified by a 3-tuple



of IP address, color, and encapsulation. Other attributes can be associated with a TLOC.

The TLOC attributes listed below can be matched or set in vSmart policies.

TLOC Attribute	Function	Application Point	
		Set By	Modify By
Address (IP address)	system-ip address of the source device on which the interface is located.	Configuration on source device	control-policy data-policy
Carrier	Identifier of the carrier type. It primarily indicates whether the transport is public or private.	Configuration on source device	control-policy
Color	Identifier of the TLOC type.	Configuration on source device	control-policy data-policy
Domain ID	Identifier of the overlay network domain.	Configuration on source device	control-policy
Encapsulation	Tunnel encapsulation, either IPsec or GRE.	Configuration on source device	control-policy data-policy
Originator	system-ip address of originating node.	Configuration on any originator	control-policy
Preference	OMP path-selection preference. A higher value is a more preferred path.	Configuration on source device	control-policy
Site ID	Identification for a give site. A site can have multiple nodes or TLOCs.	Configuration on source device	control-policy
Tag	Identifier of TLOC on any arbitrary basis.	Configuration on source device	control-policy



vRoute Attributes Used in Policies

A Viptela route, or vRoute, defines a route in the overlay network. A vRoute, which is similar to a standard IP route, has a number attributes such as TLOC and VPN. Viptela devices exchange vRoutes in OMP updates.

The vRoutes attributes listed below can be matched or set in vSmart policies.

vRoute Attribute	Function	Application Point	
		Set By	Modify By
Origin	Source of the route, either BGP, OSPF, connected, static.	Source device	control-policy
Originator	Source of the update carrying the route.	Any originator	control-policy
Preference	OMP path-selection preference. A higher value is a more preferred path.	Configuration on source device or policy	control-policy
Service	Advertised service associated with the vRoute.	Configuration on source device	control-policy
Site ID	Identifier for a give site. A site can have multiple nodes or TLOCs.	Configuration on source device	control-policy
Tag	Identification on any arbitrary basis.	Configuration on source device	control-policy
TLOC	TLOC used as next hop for the vRoute.	Configuration on source device or policy	control-policy data-policy
VPN	VPN to which the vRoute belongs.	Configuration on source device or policy	control-policy data-policy



Understanding vSmart Policy Processing and Application

Understanding how vSmart policy is processed and applied allows for proper design of policy and evaluation of how policy is being implemented across the overlay network.

Policy is processed in this way:

- A policy definition consists of a numbered, ordered sequence of match–action pairings. Within each policy, the pairings are processed in sequential order, starting with the lowest number and incrementing.
- As soon as a match occurs, the matched entity is subject to the configured action of the sequence and is then no longer subject to continued processing.
- Any entity not matched in a sequence is subject to the default action for the policy. By default, this action is reject.

vSmart policy is applied on a per-site-list basis, so:

- When applying policy to a site-list, you can apply only one of each type of policy. For example, you can have one control-policy and one data-policy, or one control-policy in and one control-policy out. You cannot have two data policies or two outbound control policies.
- Because a site-list is a grouping of many sites, you should be careful about including a site in more than one site-list, and in general, we recommend that you not do this at all. You should take special care when a site-list includes a range of site identifiers, to ensure that there is no overlap. If the same site is part of two site-lists and the same type of policy is applied to both site-lists, the policy behavior will be unpredictable and possibly catastrophic.

Control-policy is unidirectional, being applied either inbound to the vSmart controller or outbound from it. When control-policy is needed in both directions, configure two control policies. Data-policy is directional and can be applied either to traffic received from the service side of the vEdge router, traffic received from tunnel side, or both. VPN membership policy is always applied to traffic outbound from the vSmart controller.

Control-policy remains on the vSmart controller and affects routes that the controller sends and receives.

Data-policy is sent to vEdge routers in the site-list. The policy is sent in OMP updates, and it affects the data traffic that the routers send and receive.

When any node in the overlay network makes a routing decision, it uses any and all available routing information. In the overlay network, it is the vSmart controller that distributes routing information to the vEdge nodes. In a network deployment that has two or more vSmart controller, each controller acts independently to disseminate routing information to other vSmart controllers and to vEdge routers in the overlay network. So, to ensure that vSmart policy has the desired effect in the overlay network, each vSmart controller must be configured with the same policy, and the policy must be applied identically. What this means is that for any given policy, you must configure the identical policy and apply it identically across all the vSmart controllers.

Additional Information

[Configuring Centralized Control Policy](#)



