Centralized Policy

The topics in this section provide overview information about the different types of centralized policies, the components of centralized policies, and how to configure centralized policies using Cisco vManage or the CLI.

Overview of Centralized Policies

Centralized policies refer to policies that are provisioned on Cisco vSmart Controllers, which are the centralized controllers in the Cisco SD-WAN overlay network.

Types of Centralized Policies

Centralized Control Policy

Centralized control policy applies to the network-wide routing of traffic by affecting the information that is stored in the Cisco vSmart Controller's route table and that is advertised to the Cisco vEdge devices. The effects of centralized control policy are seen in how Cisco vEdge devices direct the overlay network's data traffic to its destination.

Note The centralized control policy configuration itself remains on the Cisco vSmart Controller and is never pushed to local devices.

Centralized Data Policy

Centralized data policy applies to the flow of data traffic throughout the VPNs in the overlay network. These policies can permit and restrict access based either on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol) or on VPN membership. These policies are pushed to the selected Cisco vEdge devices.

Centralized Data Policy Based on Packet Header Fields

Policy decisions affecting data traffic can be based on the packet header fields, specifically, on the source and destination IP prefixes, the source and destination IP ports, the protocol, and the DSCP.

This type of policy is often used to modify traffic flow in the network. Here are some examples of the types of control that can be effected with a centralized data policy:

- Which set of sources are allowed to send traffic to any destination outside the local site. For example, local sources that are rejected by such a data policy can communicate only with hosts on the local network.
- Which set of sources are allowed to send traffic to a specific set of destinations outside the local site. For example, local sources that match this type of data policy can send voice traffic over one path and data traffic over another.
- Which source addresses and source ports are allowed to send traffic to any destination outside the local site or to a specific port at a specific destination.

Components of Centralized Policies

The following are the components required to configure a centralized policy. Each one is explained in more detail in the sections below.

```
policy lists color-list list-name color color prefix-list list-name ip-prefix prefix
site-list list-name site-id site-id tloc-list list-name tloc address color color
encap encapsulation [preference value] vpn-list list-name vpn vpn-id
control-policy policy-name
sequence number
match match-parameters
action reject accept export-to vpn accept set parameter
default-action (accept | reject) apply-policy site-list list-name control-policy policy-name
 (in | out)
```

Components for VPN Membership

The following are the components required to configure a VPN membership policy. Each one is explained in more detail in the sections that follow.

```
policy
  lists
    app-list list-name
      (app applications | app-family application-families)
    data-prefix-list list-name
      ip-prefix prefix
    site-list list-name
      site-id site-id
    tloc-list list-name
      tloc ip-address color color encap encapsulation [preference value]
    vpn-list list-name
      vpn vpn-id
  policer policer-name
    burst bytes
    exceed action
    rate bandwidth
  data-policy policy-name
    vpn-list list-name
      sequence number
        match
          app-list list-name
          destination-data-prefix-list list-name
          destination-ip prefix/length
          destination-port port-numbers
          dscp number
          dns-app-list list-name
          dns (request | response)
          packet-length number
          protocol number
          icmp-msg
          icmp6-msg
          source-data-prefix-list list-name
          source-ip prefix/length
          source-port port-numbers
          tcp flag
        action
          cflowd (not available for deep packet inspection)
          count counter-name
          drop
          log
          redirect-dns (dns-ip-address | host)
          tcp-optimization
          accept
            nat [pool number] [use-vpn 0]
            set
              dscp number
              forwarding-class class
              local-tloc color color [encap encapsulation] [restrict]
              next-hop ip-address
              policer policer-name
              service service-name local [restrict] [vpn vpn-id]
              service service-name [tloc ip-address | tloc-list list-name] [vpn vpn-id]
              tloc ip-address color color [encap encapsulation]
              tloc-list list-name
              vpn vpn-id
      default-action
        (accept | drop)
apply-policy site-list list-name
  data-policy policy-name (all | from-service | from-tunnel)
```

Lists

A centralized data policy for deep packet inspection uses the following types of lists to group related items.

- **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Create Groups of Interest**
- **Configuration** > **Policies** > **Custom Options** > **Lists**.

Table 1:

List Type	Description	Cisco vManage	CLI Command
Applications and application families	List of one or more applications or application families running on the subnets connected to the device. *application-names* can be the names of one or more applications. The Cisco vEdge devices support about 2300 different applications. To list the supported applications, use the **?** in the CLI. *application-families* can be one or more of the following: **antivirus**, **application-service**, **audio_video**, **authentication**, **behavioral**, **compression**, **database**, **encrypted**, **erp**, **file-server**, **file-transfer**, **forum**, **game**, **instant-messaging**, **mail**, **microsoft-office**, **middleware**, **network-management**, **network-service**, **peer-to-peer**, **printer**, **routing**, **security-service**, **standard**, **telephony**, **terminal**, **thin-client**, **tunneling**, **wap**, **web**, and **webmail**.	**Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Create Groups of Interest** > **Application** or **Configuration** > **Policies** > **Centralized Policy** > **Lists** > **Application**	**app-list** *list-name* (**app** *applications* | **app-family** *application-families*)
Colors	List of one or more TLOC colors. *color* can be **3g**, **biz-internet**, **blue**, **bronze**, **custom1** through **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**. To configure multiple colors in a single list, include multiple **color** options, specifying one color in each option.		**color-list** *list-name* **color** *color*

List Type	Description	Cisco vManage	CLI Command
Prefixes	List of one or more IP prefixes. Specify the IP prefixes as follows: *prefix*/*length*—Exactly match a single prefix–length pair. **0.0.0.0/0**—Match any prefix–length pair. **0.0.0.0/0 le** *length*—Match any IP prefix whose length is less than or equal to *length*. For example, **ip-prefix 0.0.0.0/0 le 16** matches all IP prefixes with lengths from /1 through /16. **0.0.0.0/0 ge** *length*—Match any IP prefix whose length is greater than or equal to *length*. For example, **ip-prefix 0.0.0.0 ge 25** matches all IP prefixes with lengths from /25 through /32. **0.0.0.0/0 ge** *length1* **le** *length2*, or **0.0.0.0 le** *length2* **ge** *length1*—Match any IP prefix whose length is greater than or equal to *length1* and less than or equal to *length2*. For example, **ip-prefix 0.0.0.0/0 ge 20 le 24** matches all /20, /21, /22, /23, and /24 prefixes. Also, **ip-prefix 0.0.0.0/0 le 24 ge 20** matches the same prefixes. If *length1* and *length2* are the same, a single IP prefix length is matched. For example, **ip-prefix 0.0.0.0/0 ge 24 le 24** matches only /24 prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.	**Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Create Groups of Interest** > **Prefix** or **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Lists** > **Prefix**	**prefix-list** *list-name* **ip-prefix** *prefix/length*
Sites	List of one or more site identifiers in the overlay network. You can specify a single site identifier (such as **site-id 1**) or a range of site identifiers (such as **site-id 1-10**).	**Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Create Groups of Interest** > **Site** or **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Lists** > **Site**	**site-list** *list-name* **site-id** *site-id*

List Type	Description	Cisco vManage	CLI Command
TLOCs	List of one or more TLOCs in the overlay network. For each TLOC, specify its address, color, and encapsulation. *address* is the system IP address. **color** can be one of **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **mpls-restricted**, **private1** through **private6**, **public-internet**, **red**, and **silver**. *encapsulation* can be **gre** or **ipsec**. Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an **action accept** condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the lowest preference value is used. If two or more of TLOCs have the lowest preference value, traffic is sent among them in an ECMP fashion.	**Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Create Groups of Interest** > **TLOC** or **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Lists** > **Site**	**tloc-list** *list-name* **tloc** *ip-address* **color** *color* **encap** *encapsulation* [**preference** *number*]
VPNs	List of one or more VPNs in the overlay network. For data policy, you can configure any VPNs except for VPN 0 and VPN 512. To configure multiple VPNs in a single list, include multiple **vpn** options, specifying one VPN number in each option. You can specify a single VPN identifier (such as **vpn 1**) or a range of VPN identifiers (such as **vpn 1-10**).	**Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Create Groups of Interest** > **VPN** or **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Lists** > **VPN**	**vpn-list** *list-name* **vpn** *vpn-id*

VPN Lists

Each centralized data policy is associated with a VPN list. You configure VPN lists with the **policy data-policy vpn-list** command. The list you specify must be one that you created with a VPN Group of Interest or List in the Cisco vManage policy configuration wizard or with the **policy lists vpn-list** command.

For a centralized data policy, you can include any VPNs except for VPN 0 and VPN 512. VPN 0 is reserved for control traffic, so never carries any data traffic, and VPN 512 is reserved for out-of-band network management, so also never carries any data traffic. Note that while the CLI allows you to include these two VPNs in a data policy configuration, the policy is not applied to these two VPNs.

Policer Parameters

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

In Cisco vManage, you configure policer parameters from:

- **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Create Groups of Interest** > **Policer**
- **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Lists** > **Policer**

In the CLI, you configure policer parameters as follows:

```
vSmart(config)# policy policer policer-name
vSmart(config-policer)# rate bps
vSmart(config-policer)# burst bytes
vSmart(config-policer)# exceed action
```

rate is the maximum traffic rate. It can be a value from 0 through 264 – 1 bits per second.

burst is the maximum traffic burst size. It can be a value from 15000 to 1000000 bytes.

exceed is the action to take when the burst size or traffic rate is exceeded. *action* can be *drop* (the default) or *remark*. The *drop* action is equivalent to setting the packet loss priority (PLP) bit to low. The *remark* action sets the PLP bit to high. In a centralized data policy, access lists, and application-aware routing policy, you can match the PLP with the *match plp* option.

Sequences - Route or TLOC

A centralized control policy contains sequences of match–action pairs. The sequences are numbered to set the order in which a route or TLOC is analyzed by the match–action pairs in the policy.

In Cisco vManage, you configure sequences from:

- **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Configure Traffic Rules** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type**
- **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Traffic Policy** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type**

In the CLI, you configure sequences with the **policy control-policy sequence** command.

Each sequence in a centralized control policy can contain one match condition (either for a route or for a TLOC) and one action condition.

Sequences - VPN List

Each VPN list consists of sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy.

In Cisco vManage, you configure sequences from:

- **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Configure Traffic Rules** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type**
- **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Traffic Policy** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type**

In the CLI, you configure sequences with the **policy data-policy vpn-list sequence** command.

Each sequence can contain one match condition and one action condition.

Note Sequence can have either **match app-list** or **dns-app-list** configured for a policy, but not both. Configuring both **match app-list** and **dns-app-list** for a policy is not supported.

Match Parameters - Route or TLOC

A centralized control policy can match an OMP route or TLOC route attributes.

In Cisco vManage, you configure match parameters from:

- **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Configure Topology and VPN Membership** > **Add Topology** > **Custom Control (Route & TLOC)** > **Sequence Type** > **(Route | TLOC)** > **Sequence Rule** > **Match**
- **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Topology** > **Add Topology** > **Custom Control (Route & TLOC)** > **Sequence Type** > **(Route | TLOC)** > **Sequence Rule** > **Match**

Each sequence in a policy can contain one **match** section—either **match route** or **match tloc**.

Match Parameters - VPN List

A centralized data policy can match IP prefixes and fields in the IP headers, as well as applications. You can also enable split DNS.

In Cisco vManage, you configure match parameters from:

- **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Configure Traffic Rules** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type** > **Sequence Rule** > **Match**
- **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Traffic Policy** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type** > **Sequence Rule** > **Match**

Each sequence in a policy can contain one match condition.

Table 2:

Description	Cisco vManage	CLI Command	Value or Range
Match all packets	**Omit Match**	**omit match** command	—
Applications or application families	**Match Applications/Application Family List**	**app-list** *list-name*	Name of an application list or an **app-list** *list*
Group of destination prefixes	**Match Destination Data Prefix**	**destination-data-prefix-list** *list-name*	Name of a data prefix list or a **data-prefix-list** *list*
Individual destination prefix	**Match Destination Data Prefix**	**destination-ip** *prefix*/length	IP prefix and prefix length

Description	Cisco vManage	CLI Command	Value or Range
Destination port number	**Match Destination Port**	**destination-port** *number*	0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])
Enable split DNS, to resolve and process DNS requests and responses on an application-by-application basis	**Match DNS Application List**	**dns-app-list** *list-name*	Name of an **app-list** *list*. This list specifies the applications whose DNS requests are processed.
Specify the direction in which to process DNS packets	**Match DNS**	**dns (request |response)**	To process DNS requests sent by the applications (for outbound DNS queries), specify **dns request**. To process DNS responses returned from DNS servers to the applications, specify **dns response**.
DSCP value	**Match DSCP**	**dscp** *number*	0 through 63
Packet length	**Match Packet Length**	**packet-length** *number*	0 through 65535; specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-])
Packet loss priority (PLP)	**Match PLP**	**plp**	(**high | low**) By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.
Internet protocol number	**Match Protocol**	**protocol** *number*	0 through 255
For Protocol IPv4 when you enter a Protocol value as 1, the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. Likewise, the **ICMP Message** field displays for Protocol IPv6 when you enter a Protocol value as 58. When you select Protocol as Both, the **ICMP Message or ICMPv6 Message** field displays. **Note** This field is available from , Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1.	**ICMP Message** **ICMP Message** or **ICMPv6 Message**	**icmp-msg** *value* **icmp6-msg** *value*	For **icmp-msg** message type, refer to the table below for ICMP Message Types/Codes and Corresponding Enumeration Values. For **icmp6-msg message** type, refer to the table below for ICMPv6 Message Types/Codes and Corresponding Enumeration Values.

Description	Cisco vManage	CLI Command	Value or Range
Group of source prefixes	**Match Source Data Prefix**	**source-data-prefix-list** *list-name*	Name of a data prefix or a **data-prefix-list** *list*
Individual source prefix	**Match Source Data Prefix**	**source-ip** prefix/length	IP prefix and prefix length
Source port number	**Match Source Port**	**source-port** *address*	0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])
TCP flag	—	**tcp** *flag*	**syn**

Table 3: ICMP Message Types/Codes and Corresponding Enumeration Values

Type	Code	Enumeration
0	0	echo-reply
3		unreachable
	0	net-unreachable
	1	host-unreachable
	2	protocol-unreachable
	3	port-unreachable
	4	packet-too-big
	5	source-route-failed
	6	network-unknown
	7	host-unknown
	8	host-isolated
	9	dod-net-prohibited
	10	dod-host-prohibited
	11	net-tos-unreachable
	12	host-tos-unreachable
	13	administratively-prohibited
	14	host-precedence-unreachable
	15	precedence-unreachable

5		redirect
	0	net-redirect
	1	host-redirect
	2	net-tos-redirect
	3	host-tos-redirect
8	0	echo
9	0	router-advertisement
10	0	router-solicitation
11		time-exceeded
	0	ttl-exceeded
	1	reassembly-timeout
12		parameter-problem
	0	general-parameter-problem
	1	option-missing
	2	no-room-for-option
13	0	timestamp-request
14	0	timestamp-reply
40	0	photuris
42	0	extended-echo
43		extended-echo-reply
	0	echo-reply-no-error
	1	malformed-query
	2	interface-error
	3	table-entry-error
	4	multiple-interface-match

Table 4: ICMPv6 Message Types/Codes and Corresponding Enumeration Values

Type	Code	Enumeration

1		unreachable
	0	no-route
	1	no-admin
	2	beyond-scope
	3	destination-unreachable
	4	port-unreachable
	5	source-policy
	6	reject-route
	7	source-route-header
2	0	packet-too-big
3		time-exceeded
	0	hop-limit
	1	reassembly-timeout
4		parameter-problem
	0	Header
	1	next-header
	2	parameter-option
128	0	echo-request
129	0	echo-reply
130	0	mld-query
131	0	mld-report
132	0	mld-reduction
133	0	router-solicitation
134	0	router-advertisement
135	0	nd-ns
136	0	nd-na
137	0	redirect
138		router-renumbering
	0	renum-command
	1	renum-result
	255	renum-seq-number

139		ni-query
	0	ni-query-v6-address
	1	ni-query-name
	2	ni-query-v4-address
140		ni-response
	0	ni-response-success
	1	ni-response-refuse
	2	ni-response-qtype-unknown
141	0	ind-solicitation
142	0	ind-advertisement
143		mldv2-report
144	0	dhaad-request
145	0	dhaad-reply
146	0	mpd-solicitation
147	0	mpd-advertisement
148	0	cp-solicitation
149	0	cp-advertisement
151	0	mr-advertisement
152	0	mr-solicitation
153	0	mr-termination
155	0	rpl-control

OMP Route Match Attributes

For OMP routes (vRoutes), you can match these attributes:

Table 5:

Description	Cisco vManage	CLI Command	Value or Range
Individual color.	Not available in Cisco vManage.	**color** *color*	**3g**, **biz-internet**, **blue**, **bronze**, **custom1** through **custom3**,**default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**
One or more colors.	**Match Color List**	**color-list** *list-name*	Name of a color or a **policy lists color-list** list.

Description	Cisco vManage	CLI Command	Value or Range
Tag value associated with the route or prefix in the routing database on the device.	**Match OMP Tag**	**omp-tag** *number*	0 through 4294967295
Protocol from which the route was learned.	**Match Origin**	**origin** *protocol*	**bgp-external**, **bgp-internal**, **connected**, **ospf-external1**, **ospf-external2**, **ospf-inter-area**, **ospf-intra-area**, **static**
IP address from which the route was learned.	**Match Originator**	**originator** *ip-address*	IP address
How preferred a prefix is. This is the preference value that the route or prefix has in the local site, that is, in the routing database on the device. A higher preference value is more preferred.	**Match Preference**	**preference** *number*	0 through 255
One or more prefixes.	**Match Prefix List**	**prefix-list** *list-name*	Name of a prefix list or a **policy lists prefix-list** list.
Individual site identifier.	Not available in Cisco vManage.	**site-id** *site-id*	0 through 4294967295
One or more overlay network site identifiers.	**Match Site**	**site-list** *list-name*	Name of a site or a **policy lists site-list** list.
Individual TLOC address.	**Match TLOC**	**tloc** *ip-address*	IP address
One or more TLOC addresses.	**Match TLOC**	**tloc-list** *list-name*	Name of a TLOC or a **policy lists tloc-list** list.
Individual VPN identifier.	**Match VPN**	**vpn** *vpn-id*	0 through 65535
One or more VPN identifiers.	**Match VPN**	**vpn-list** *list-name*	Name of a VPN or a **policy lists vpn-list** list.

In the CLI, you configure the OMP route attributes to match with the **policy control-policy sequence match route** command, and you configure the TLOC attributes to match with the **policy control-policy sequence match tloc** command.

TLOC Route Match Attributes

For TLOC routes, you can match these attributes:

Table 6:

Description	Cisco vManage	CLI Command	Value or Range
Carrier for the control traffic.	**Match Carrier**	**carrier** *carrier-name*	**default**, **carrier1** through **carrier8**

Description	Cisco vManage	CLI Command	Value or Range
Individual color.	Not available in Cisco vManage.	**color** *color*	**3g**, **biz-internet**, **blue**, **bronze**, **custom1** through **custom3**,**default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**
One or more colors.	**Match Color List**	**color-list** *list-name*	See the colors above.
Domain identifier associated with a TLOC.	**Match Domain ID**	**domain-id** *domain-id*	0 through 4294967295
Tag value associated with the TLOC route in the route table on the device.	**Match OMP Tag**	**omp-tag** *number*	0 through 4294967295
IP address from which the route was learned.	**Match Originator**	**originator** *ip-address*	IP address
How preferred a TLOC route is. This is the preference value that the TLOC route has in the local site, that is, in the route table on the Cisco SD-WAN device. A higher preference value is more preferred.	**Match Preference**	**preference** *number*	0 through 255
Individual site identifier.	**Match Site**	**site-id** *site-id*	0 through 4294967295
One or more overlay network site identifiers.	**Match Site**	**site-list** *list-name*	Name of a **policy lists site-list** list.
Individual TLOC address.	**Match TLOC**	**tloc** *address*	IP address
One or more TLOC addresses.	**Match TLOC**	**tloc-list** *list-name*	Name of a **policy lists tloc-list** list.

Action Parameters - Route or TLOC

For each match condition, you configure a corresponding action to take if the route or TLOC matches.

In Cisco vManage, you configure match parameters from:

- **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Configure Topology and VPN Membership** > **Add Topology** > **Custom Control (Route & TLOC)** > **Sequence Type > (Route | TLOC)** > **Sequence Rule** > **Action**
- **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Topology** > **Add Topology** > **Custom Control (Route & TLOC)** > **Sequence Type > (Route | TLOC)** > **Sequence Rule** > **Action**

In the CLI, you configure actions with the **policy control-policy action** command.

Each sequence in a centralized control policy can contain one action condition.

In the action, you first specify whether to accept or reject a matching route or TLOC:

Table 7:

Description	Cisco vManage	CLI Command	Value or Range
Accept the route. An accepted route is eligible to be modified by the additional parameters configured in the **action** portion of the policy configuration.	Click **Accept**.	**accept**	—
Discard the packet.	Click **Reject**.	**reject**	—

Then, for a route or TLOC that is accepted, you can configure the following actions:

Table 8:

Description	Cisco vManage	CLI Command	Value or Range
Export the route the the specified VPN or list of VPNs (for a **match route** match condition only).	Click **Accept**, then action **Export To**.	**export-to** (**vpn** *vpn-id* | **vpn-list** *vpn-list*)	0 through 65535 or list name.
Change the tag string in the route, prefix, or TLOC.	Click **Accept**, then action **OMP Tag**.	**set omp-tag** *number*	0 through 4294967295
Change the preference value in the route, prefix, or TLOC to the specified value. A higher preference value is more preferred.	Click **Accept**, then action **Preference**.	**set preference** *number*	0 through 255
Specify a service to redirect traffic to before delivering the traffic to its destination. The TLOC address or list of TLOCs identifies the TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Configure the services themselves on the Cisco SD-WAN devices that are collocated with the service devices, using the **vpn service** configuration command.	Click **Accept**, then action **Service**.	**set service** *service-name* (**tloc** *ip-address* | **tloc-list** *list-name*) [**vpn** *vpn-id*]	Standard services: **FW**, **IDS**, **IDP** Custom services: **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4** TLOC list configured with a **policy lists tloc-list** command.
Change the TLOC address, color, and encapsulation to the specified address and color.	Click **Accept**, then action **TLOC**.	**set tloc** *ip-address* **color** *color* [**encap** *encapsulation*]	IP address, TLOC color, and encapsulation, Color can be one of **3g**, **biz-internet**, **blue**, **bronze**, **custom1** through **custom3**,**default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**. Encapsuation can be either **gre** or **ipsec**.

Description	Cisco vManage	CLI Command	Value or Range
Direct matching routes or TLOCs using the mechanism specified by *action*, and enable end-to-end tracking of whether the ultimate destination is reachable. Setting a TLOC action is useful when traffic is first directed, via policy, to an intermediate destination, which then forwards the traffic to its ultimate destination. For example, for traffic from vEdge-A destined for vEdge-D, a policy might direct traffic from vEdge-A first to vEdge-B (the intermediate destination), and vEdge-B then sends it to the final destination, vEdge-D. Setting the TLOC action option enables the Cisco vSmart Controller to perform end-to-end tracking of the path to the ultimate destination device. In our example, matching traffic goes from vEdge-A to vEdge-B and then, in a single hop, goes to vEdge-D. If the tunnel between vEdge-B and vEdge-D goes down, the Cisco vSmart Controller relays this information to vEdge-A, and vEdge-A removes its route to vEdge-D from its local route table. End-to-end tracking works here only because traffic goes from vEdge-B to vEdge-D in a single hop, using a single tunnel. If the traffic from vEdge-A went first to vEdge-B, then to vEdge-C, and finally to vEdge-D, the Cisco vSmart Controller is unable to perform end-to-end tracking and is thus unable to keep vEdge-A informed about whether full path between it and vEdge-D is up.	Click **Accept**, then action **TLOC Action**.	**set tloc-action** *action*	**ecmp**—Equally direct matching control traffic between the intermediate destination and the ultimate destination. In our example, traffic would be sent to vEdge-B (which would then send it to vEdge-D) and directly to vEdge-D. With this action, if the intermediate destination is down, all traffic reaches the ultimate destination. **primary**—First direct matching traffic to the intermediate destination. If that device is not reachable, then direct it to the final destination. In our example, traffic would first be sent to vEdge-B. If this device is down, it is sent directly to vEdge-D. With this action, if the intermediate destination is down, all traffic reaches the final destination. **backup**—First direct matching traffic to the final destination. If that device is not reachable, then direct it to the intermediate destination. In our example, traffic would first be sent directly to vEdge-D. If the vEdge-A is not able to reach vEdge-D, traffic is sent to vEdge-B, which might have an operational path to reach vEdge-D. With this action, if the source is unable to reach the final destination directly, it is possible for all traffic to reach the final destination via the intermediate destination. **strict**—Direct matching traffic only to the intermediate destination. In our example, traffic is sent only to vEdge-B, regardless of whether it is reachable. With this action, if the intermediate destination is down, no traffic reaches the final destination. If you do not configure a set tloc-action in a centralized control policy, strict is the default behavior.
Change the TLOC address and color to those in the specified TLOC list.	Click **Accept**, then action **TLOC**.	**set tloc-list** *list-name*	Name of a **policy lists tloc-list** list.

Action Parameters - VPN List

Table 9: Feature History

Feature Name	Release Information	Description
Path Preference Support for Cisco IOS XE SD-WAN Devices	Cisco IOS XE Release 17.2.1r	This feature extends to Cisco IOS XE SD-WAN devices, support for selecting one or more local transport locators (TLOCs) for a policy action.
Traffic Redirection to SIG Using Data Policy	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	With this feature, while creating a data policy, you can define an application list along with other match criteria and redirect the application traffic to a Secure Internet Gateway (SIG).

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped, and it can be counted. Then, you can associate parameters with accepted packets.

In Cisco vManage, you configure match parameters from:

- **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Configure Traffic Rules** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type** > **Sequence Rule** > **Action**
- **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Traffic Policy** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type** > **Sequence Rule** > **Action**.

In the CLI, you configure the action parameters with the **policy data-policy vpn-list sequence action** command.

Each sequence in a centralized data policy can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

Table 10:

Description	Cisco vManage	CLI Command	Value or Range
Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.	Click **Accept**	**accept**	—
Enable cflowd traffic monitoring.	Click **Accept**, then action **Cflowd**	**cflowd**	—
Count the accepted or dropped packets.	Action Counter Click **Accept**, then action **Counter**	**count** *counter-name*	Name of a counter. Use the **show policy access-lists counters** command on the Cisco vEdge device.
Discard the packet. This is the default action.	Click **Drop**	**drop**	—

Description	Cisco vManage	CLI Command	Value or Range
Log the packet. Packets are placed into the messages and vsyslog system logging (syslog) files.	**Action Log** Click **Accept**, then action **Log**	**log**	To view the packet logs, use the **show app log flows** and **show log** commands.
Redirect DNS requests to a particular DNS server. Redirecting requests is optional, but if you do so, you must specify both actions.	Click **Accept**, then action **Redirect DNS**	**redirect-dns hostredirect-dns** *ip-address*	For an inbound policy, **redirect-dns host** allows the DNS response to be correctly forwarded back to the requesting service VPN. For an outbound policy, specify the IP address of the DNS server.
Fine-tune TCP to decrease round-trip latency and improve throughout for matching TCP traffic.	Click **Accept**, then action **TCP Optimization**	**tcp-optimization**	—
Redirect application traffic to a SIG Note: Before you apply a data policy for redirecting application traffic to a SIG, you must have configured the SIG tunnels. For more information on configuring Automatic SIG tunnels, see Automatic Tunnels. For more information on configuring Manual SIG tunnels, see Manual Tunnels.	Click **Accept**, then action **Secure Internet Gateway**	**sig**	—

Then, for a packet that is accepted, the following parameters can be configured:

Table 11:

Description	Cisco vManage	CLI Command	Value or Range
Enable cflowd traffic monitoring.	Click **Accept**, then action **Cflowd**.	**cflowd**	—
Direct matching traffic to the NAT functionality so that it can be redirected directly to the Internet or other external destination.	Click **Accept**, then action **NAT Pool** or **NAT VPN**.	**nat** [**pool** *number*] [**use-vpn 0**]	—
DSCP value.	Click **Accept**, then action **DSCP**.	**set dscp** *value*	0 through 63
Forwarding class.	Click **Accept**, then action **Forwarding Class**.	**set forwarding-class** *value*	Name of forwarding class

Description	Cisco vManage	CLI Command	Value or Range
Direct matching packets to a TLOC that mathces the color and encapsulation By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC.	Click **Accept**, then action **Local TLOC**.	**set local-tloc color** *color* [**encap** *encapsulation*]	*color* can be: **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**. By default, *encapsulation* is **ipsec**. It can also be **gre**.
Direct matching packets to one of the TLOCs in the list if the TLOC matches the color and encapsulation By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the **restrict** option.	Click **Accept**, then action **Local TLOC**	**set local-tloc-list color** *color* **encap** *encapsulation* [**restrict**]	
Set the next hop to which the packet should be forwarded.	Click **Accept**, then action **Next Hop**.	**set next-hop** *ip-address*	IP address
Apply a policer.	Click **Accept**, then action **Policer**.	**set policer** *policer-name*	Name of policer configured with a **policy policer** command.
Specify a service to redirect traffic to before delivering the traffic to its destination. The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Configure the services themselves on the Cisco vEdge devices that are collocated with the service devices, using the **vpn service** command.	Click **Accept**, then action **Service**.	**set service** *service-name* [**tloc** *ip-address* | **tloc-list** *list-name*] [**vpn** *vpn-id*]	Standard services: **FW**, **IDS**, **IDP** Custom services: **netsvc1**, **netsvc2**,**netsvc3**, **netsvc4** TLOC list is configured with a **policy lists tloc-list** list.
Direct traffic to a remote TLOC that matches the IP address, color, and encapsulation.	Click **Accept**, then action **TLOC**.	**set tloc** *address* **color** *color* [**encap** *encapsulation*]	TLOC address, color, and encapsulation
Direct traffic to one of the remote TLOCs in the TLOC list if it matches the IP address, color, and encapsulation of one of the TLOCs in the list. If a preference value is configured for the matching TLOC, that value is assigned to the traffic.	Click **Accept**, then action **TLOC**.	**set tloc-list** *list-name*	Name of a **policy lists tloc-list** list
Set the VPN that the packet is part of.	Click **Accept**, then action **VPN**.	**set vpn** *vpn-id*	0 through 65530

The following table describes the IPv4 and IPv6 actions.

Table 12:

IPv4 Actions	IPv6 Actions
drop, dscp, next-hop (from-service only)/vpn, count, forwarding class, policer (only in interface ACL), App-route SLA (only)	N/A
App-route preferred color, app-route sla strict, cflowd, nat, redirect-dns	N/A
N/A	drop, dscp, next-hop/vpn, count, forwarding class, policer (only in interface ACL) App-route SLA (only), App-route preferred color, app-route sla strict
policer (DataPolicy), tcp-optimization, fec-always,	policer (DataPolicy)
tloc, tloc-list (set tloc, set tloc-list)	tloc, tloc-list (set tloc, set tloc-list)
App-Route backup-preferred color, local-tloc, local-tloc-list	App-Route backup-preferred color, local-tloc, local-tloc-list

Default Action - Route or TLOC

If a route or TLOC being evaluated does not match any of the match conditions in a centralized control policy, a default action is applied to it. By default, the route or TLOC is rejected.

In Cisco vManage, you modify the default action from **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Configure Topology and VPN Membership** > **Add Topology** > **Custom Control (Route and TLOC)** > **Sequence Type** > **(Route | TLOC)** > **Sequence Rule** > **Default Action**.

In the CLI, you modify the default action with the **control policy default-action accept** command.

Default Action - VPN List

If a data packet being evaluated does not match any of the match conditions in a data policy, a default action is applied to the packet. By default, the data packet is dropped

In Cisco vManage, you modify the default action from:

- **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Configure Traffic Rules** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type** > **Sequence Rule** > **Default Action**
- **Configuration** > **Policies** > **Custom Options** > **Centralized Policy** > **Traffic Policy** > **(Application-Aware Routing | Traffic Data | Cflowd)** > **Sequence Type** > **Sequence Rule** > **Default Action**.

In the CLI, you modify the default action with the **policy data-policy vpn-list default-action accept** command.

Configure Centralized Policies Using Cisco vManage

To configure a centralized policy, use the Cisco vManage policy configuration wizard. The wizard consists of the following operations that guide you through the process of creating and editing policy components:

- Create Groups of Interest—Create lists that group together related items and that you call in the match or action components of a policy.
- Configure Topology and VPN Membership—Create the network structure to which the policy applies.
- Configure Traffic Rules—Create the match and action conditions of a policy.
- Apply Policies to Sites and VPNs—Associate the policy with sites and VPNs in the overlay network.
- Activate the centralized policy.

  For a centralized policy to take effect, you must activate the policy.

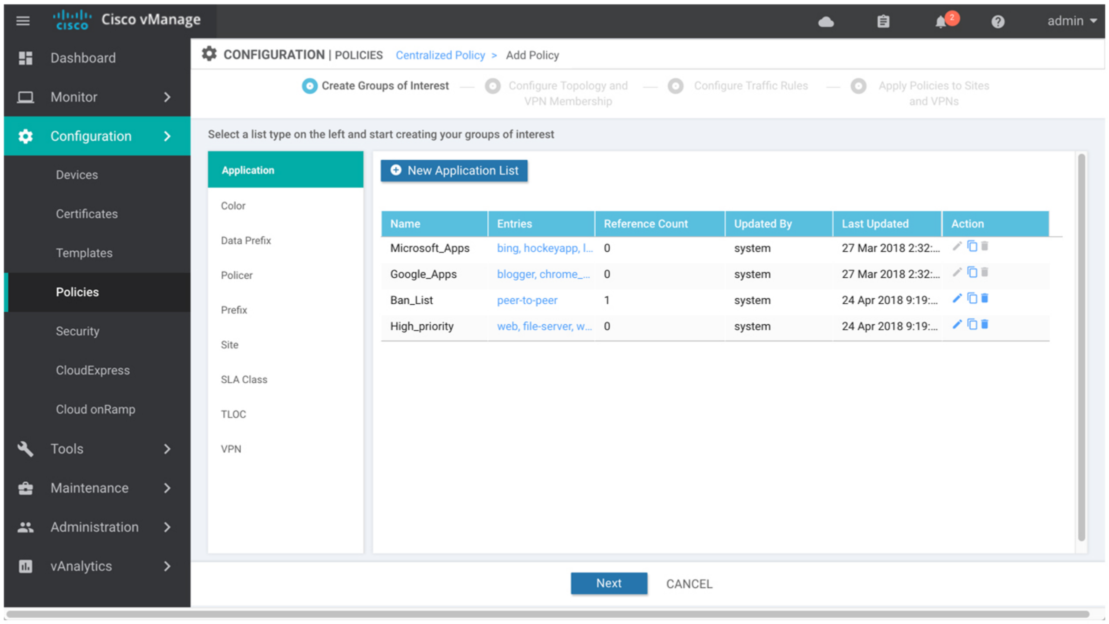
Start the Policy Configuration Wizard

1. In Cisco vManage, select the **Configuration** > **Policies** screen.
2. Select the **Centralized Policy** tab.
3. Click **Add Policy**.

The policy configuration wizard appears, and the **Create Groups of Interest** screen is displayed.

Configure Groups of Interest

In **Create Groups of Interest**, create lists of groups to use in a centralized policy:



Select a list type on the left and start creating your groups of interest

Name	Entries	Reference Count	Updated By	Last Updated	Action
Microsoft_Apps	bing, hockeyapp, l...	0	system	27 Mar 2018 2:32:...	
Google_Apps	blogger, chrome_...	0	system	27 Mar 2018 2:32:...	
Ban_List	peer-to-peer	1	system	24 Apr 2018 9:19:...	
High_priority	web, file-server, w...	0	system	24 Apr 2018 9:19:...	

1. Create new lists as described in the following table:

Table 13:

List Type	Procedure
Application	**a.** In the left bar, click **Application**. **b.** Click **New Application List**. **c.** Enter a name for the list. **d.** Click either the **Application** or **Application Family** button. **e.** From the **Select** drop-down, select the desired applications or application families. **f.** Click **Add**. Two application lists are preconfigured. You cannot edit or delete these lists. • **Microsoft_Apps**—Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the Entries column. • **Google_Apps**—Includes Google applications, such as gmail, Google maps, and YouTube. To display a full list of Google applications, click the list in the Entries column.
Color	**a.** In the left bar, click **Color**. **b.** Click **New Color List**. **c.** Enter a name for the list. **d.** From the **Select Color** drop-down, select the desired colors. **e.** Click **Add**.
Data Prefix	**a.** In the left bar, click **Data Prefix**. **b.** Click **New Data Prefix List**. **c.** Enter a name for the list. **d.** Select either **IPv4** or **IPv6**. **e.** In the **Add Data Prefix** field, enter one or more data prefixes separated by commas. **f.** Click **Add**.

List Type	Procedure
Policer	**a.** In the left bar, click **Policer**. **b.** Click **New Policer List**. **c.** Enter a name for the list. **d.** Define the policing parameters: **1.** In the **Burst** field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes. **2.** In the **Exceed** field, select the action to take when the burst size or traffic rate is exceeded. It can be **drop**, which sets the packet loss priority (PLP) to **low**. You can use the **remark** action to set the packet loss priority (PLP) to **high**. **3.** In the **Rate** field, enter the maximum traffic rate, a value from 0 through $2^{64} – 1$ bits per second (bps). **e.** Click **Add**.
Prefix	**a.** In the left bar, click **Prefix**. **b.** Click **New Prefix List**. **c.** Enter a name for the list. **d.** In the **Add Prefix** field, enter one or more data prefixes separated by commas. **e.** Click **Add**.
Site	**a.** In the left bar, click **Site**. **b.** Click **New Site List**. **c.** Enter a name for the list. **d.** In the **Add Site** field, enter one or more site IDs separated by commas. **e.** Click **Add**.

List Type	Procedure
SLA Class	**a.** In the left bar, click **SLA Class**. **b.** Click **New SLA Class List**. **c.** Enter a name for the list. **d.** Define the SLA class parameters: **1.** In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent. **2.** In the **Latency** field, enter the maximum packet latency on the connection, a value from 0 through 1,000 milliseconds. **3.** In the **Jitter** field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds. **e.** Click **Add**.
TLOC	**a.** In the left bar, click **TLOC**. **b.** Click **New TLOC List**. The **TLOC List** popup displays. **c.** Enter a name for the list. **d.** In the **TLOC IP** field, enter the system IP address for the TLOC. **e.** In the **Color** field, select the TLOC's color. **f.** In the **Encap** field, select the encapsulation type. **g.** In the **Preference** field, optionally select a preference to associate with the TLOC. **h.** Click **Add TLOC** to add another TLOC to the list. **i.** Click **Save**.
VPN	**a.** In the left bar, click **VPN**. **b.** Click **New VPN List**. **c.** Enter a name for the list. **d.** In the **Add VPN** field, enter one or more VPN IDs separated by commas. **e.** Click **Add**.

2. Click **Next** to move to **Configure Topology and VPN Membership** in the wizard.

Configure Topology and VPN Membership

When you first open the **Configure Topology and VPN Membership** screen, the **Topology** tab is selected by default.

To configure topology and VPN membership:

Hub-and-Spoke

1. In the **Add Topology** drop-down, select **Hub-and-Spoke**.
2. Enter a name for the hub-and-spoke policy.
3. Enter a description for the policy.
4. In the **VPN List** field, select the VPN list for the policy.
5. In the left pane, click **Add Hub-and-Spoke**. A hub-and-spoke policy component containing the text string **My Hub-and-Spoke** is added in the left pane.
6. Double-click the **My Hub-and-Spoke** text string, and enter a name for the policy component
7. In the right pane, add hub sites to the network topology:
    a. Click **Add Hub Sites**.
    b. In the **Site List** field, select a site list for the policy component.
    c. Click **Add**.
    d. Repeat these steps to add more hub sites to the policy component.
8. In the right pane, add spoke sites to the network topology:
    a. Click **Add Spoke Sites**.
    b. In the **Site List Field**, select a site list for the policy component.
    c. Click **Add**.
    d. Repeat these steps to add more spoke sites to the policy component.
9. Repeat steps as needed to add more components to the hub-and-spoke policy.
10. Click **Save Hub-and-Spoke Policy**.

Mesh

1. In the **Add Topology** drop-down, select **Mesh**.
2. Enter a name for the mesh region policy component.
3. Enter a description for the mesh region policy component.
4. In the **VPN List** field, select the VPN list for the policy.
5. Click **New Mesh Region**.
6. In the **Mesh Region Name** field, enter a name for the individual mesh region.
7. In the **Site List** field, select one or more sites to include in the mesh region.
8. Click **Add**.
9. Repeat these steps to add more mesh regions to the policy.
10. Click **Save Mesh Topology**.

Custom Control (Route & TLOC): Centralized route control policy (for matching OMP routes)

1. In the **Add Topology** drop-down, select **Custom Control (Route & TLOC)**.
2. Enter a name for the control policy.
3. Enter a description for the policy.
4. In the left pane, click **Sequence Type**. The **Add Custom Control Policy** popup displays.
5. Select **Route**. A policy component containing the text string **Route** is added in the left pane.
6. Double-click the **Route** text string, and enter a name for the policy component.
7. In the right pane, click **Sequence Rule**. The **Match/Actions** box opens, and **Match** is selected by default.
8. From the boxes under the **Match** box, select the desired policy match type. Then select or enter the value for that match condition. Configure additional match conditions for the sequence rule, as desired.
9. Click **Actions**. The **Reject** radio button is selected by default. To configure actions to perform on accepted packets, click the **Accept** radio button. Then select the action or enter a value for the action.
10. Click **Save Match and Actions**.
11. Click **Sequence Rule** to configure more sequence rules, as desired. Drag and drop to re-order them.
12. Click **Sequence Type** to configure more sequences, as desired. Drag and drop to re-order them.
13. Click **Save Control Policy**.

Custom Control (Route & TLOC): Centralized TLOC control policy (for matching TLOC routes)

1. In the **Add Topology** drop-down, select **Custom Control (Route & TLOC)**.
2. Enter a name for the control policy.
3. Enter a description for the policy.
4. In the left pane, click **Sequence Type**. The **Add Custom Control Policy** popup displays.
5. Select **TLOC**. A policy component containing the text string **TLOC** is added in the left pane.
6. Double-click the **TLOC** text string, and enter a name for the policy component.
7. In the right pane, click **Sequence Rule**. The **Match/Actions** box opens, and **Match** is selected by default.
8. From the boxes under the **Match** box, select the desired policy match type. Then select or enter the value for that match condition. Configure additional match conditions for the sequence rule, as desired.
9. Click **Actions**. The **Reject** radio button is selected by default. To configure actions to perform on accepted packets, click the **Accept** radio button. Then select the action or enter a value for the action.
10. Click **Save Match and Actions**.
11. Click **Sequence Rule** to configure more sequence rules, as desired. Drag and drop to re-order them.
12. Click **Sequence Type** to configure more sequences, as desired. Drag and drop to re-order them.
13. Click **Save Control Policy**.

Import Existing Topology

1. In the **Add Topology** drop-down, click **Import Existing Topology**. The **Import Existing Topology** popup appears.
2. Select the type of topology.
3. For **Policy Type**, choose the name of the topology you want to import.
4. In the **Policy** drop-down, select a policy to import.
5. Click **Import**.

Click **Next** to move to **Configure Traffic Rules** in the wizard.

Create a VPN Membership Policy

1. In the **Topology** bar, click **VPN Membership**.
2. Click **Add VPN Membership Policy**.

   The **Update VPN Membership Policy** popup displays.
3. Enter a name and description for the VPN membership policy.
4. In the **Site List** field, select the site list.
5. In the **VPN Lists** field, select the VPN list.
6. Click **Add List** to add another VPN to the VPN membership.
7. Click **Save**.
8. Click **Next** to move to **Configure Traffic Rules** in the wizard.

Configure Traffic Rules

Table 14: Feature History

Feature Name	Release Information	Description
Policy Matching with ICMP Message	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This feature provides support for a new match condition that you can use to specify a list of ICMP messages for centralized data policies, localized data policies, and Application-Aware Routing policies.

When you first open the **Configure Traffic Rules** screen, the **Application-Aware Routing** tab is selected by default. For more information on configuring traffic rules for deep packet inspection, see Deep Packet Inspection.

To configure traffic rules for a centralized data policy:

1. Click the **Traffic Data** tab.
2. Click the **Add Policy** drop-down.
3. Click **Create New**. The **Add Data Policy** screen displays.

4. Enter a name and a description for the data policy.
5. In the right pane, click **Sequence Type**. The **Add Data Policy** popup opens.
6. Select the type of data policy you want to create, **Application Firewall**, **QoS**, **Service Chaining**, **Traffic Engineering**, or **Custom**.
7. A policy sequence containing the text string **Application**, **Firewall**, **QoS**, **Service Chaining**, **Traffic Engineering**, or **Custom** is added in the left pane.
8. Double-click the text string, and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.
9. In the right pane, click **Sequence Rule**. The **Match/Action** box opens, and **Match** is selected by default. The available policy match conditions are listed below the box.

Match Condition	Procedure	IPv4 Fields	IPv6 Fields
None (match all packets)	Do not specify any match conditions.	—	—
Applications /Application Family List	**a.** In the **Match** conditions, click **Applications/Application Family List**. **b.** In the drop-down, select the application family. **c.** To create an application list: **1.** Click **New Application List**. **2.** Enter a name for the list. **3.** Click **Application** to create a list of individual applications. Click **Application Family** to create a list of related applications. **4.** In the **Select Application** drop-down, select the desired applications or application families. **5.** Click **Save**.	app-list	—
Destination Data Prefix	**a.** In the **Match** conditions, click **Destination Data Prefix**. **b.** To match a list of destination prefixes, select the list from the drop-down. **c.** To match an individual destination prefix, enter the prefix in the **Destination: IP Prefix** field.	source/ destination-data-prefix-list	source/ destination-data-prefix-list

Match Condition	Procedure	IPv4 Fields	IPv6 Fields
Destination Port	**a.** In the **Match** conditions, click **Destination Port**. **b.** In the **Destination: Port** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).	src/dst ip	src/dst ip
DNS Application List	Add an application list to enable split DNS. **a.** In the **Match** conditions, click **DNS Application List**. **b.** In the drop-down, select the application family.	dns-app-list	—
DNS	Add an application list to process split DNS. **a.** In the **Match** conditions, click **DNS**. **b.** In the drop-down, select **Request** to process DNS requests for the DNS applications, and select **Response** to process DNS responses for the applications.	dns-request dns-response	—
DSCP	**a.** In the **Match** conditions, click **DSCP**. **b.** In the **DSCP** field, type the DSCP value, a number from 0 through 63.	dscp	dscp
Packet Length	**a.** In the **Match** conditions, click **Packet Length**. **b.** In the **Packet Length** field, type the length, a value from 0 through 65535.	packet-len	packet-len
PLP	**a.** In the **Match** conditions, click **PLP** to set the **Packet Loss Priority**. **b.** In the **PLP** drop-down, select **Low** or **High**. To set the PLP to **High**, apply a policer that includes the **exceed remark** option.	—	—
Protocol	**a.** In the **Match** conditions, click **Protocol**. **b.** In the **Protocol** field, type the Internet Protocol number, a number from 0 through 255.	Protocol	Protocol
ICMP Message	To match ICMP messages, in the Protocol field, set the Internet Protocol Number to 1, or 58, or both. **Note** This field is available from , Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1.	ICMP Message	ICMP Message

Match Condition	Procedure	IPv4 Fields	IPv6 Fields
Source Data Prefix	**a.** In the **Match** conditions, click **Source Data Prefix**. **b.** To match a list of source prefixes, select the list from the drop-down. **c.** To match an individual source prefix, enter the prefix in the **Source** field.	source/ destination-data-prefix-list	source /destination-data-prefix-list
Source Port	**a.** In the **Match** conditions, click **Source Port**. **b.** In the **Source** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).	ports	ports
TCP	**a.** In the **Match** conditions, click **TCP**. **b.** In the **TCP** field, **syn** is the only option available.	tcp flag	—

10. For QoS and Traffic Engineering data policies: From the **Protocol** drop-down list, select **IPv4** to apply the policy only to IPv4 address families, **IPv6** to apply the policy only to IPv6 address families, or **Both** to apply the policy to IPv4 and IPv6 address families.

11. To select one or more **Match** conditions, click its box and set the values as described.

Note Not all match conditions are available for all policy sequence types.

12. To select actions to take on matching data traffic, click the **Actions** box.

13. To drop matching traffic, click **Drop**. The available policy actions are listed to the right of the button.

14. To accept matching traffic, click **Accept**. The available policy actions are listed to the right of the button.

15. Set the policy action as described.

Note Not all actions are available for all match conditions.

Match Condition	Description	Procedure
Counter	Count matching data packets.	**a.** In the **Action** conditions, click **Counter**. **b.** In the **Counter Name** field, enter the name of the file in which to store packet counters.

Match Condition	Description	Procedure
DSCP	Assign a DSCP value to matching data packets.	**a.** In the **Action** conditions, click **DSCP**. **b.** In the **DSCP** field, type the DSCP value, a number from 0 through 63.
Forwarding Class	Assign a forwarding class to matching data packets.	**a.** In the **Match** conditions, click **Forwarding Class**. **b.** In the **Forwarding Class** field, type the class value, which can be up to 32 characters long.
Log	Place a sampled set of packets that match the SLA class rule into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.	**a.** In the **Action** conditions, click **Log** to enable logging.
Policer	Apply a policer to matching data packets.	**a.** In the **Match** conditions, click **Policer**. **b.** In the **Policer** drop-down field, select the name of a policer.

Match Condition	Description	Procedure
Loss Correction	Apply loss correction to matching data packets. Forward Error Correction (FEC) recovers lost packets on a link by sending redundant data, enabling the receiver to correct errors without the need to request retransmission of data. FEC is supported only for IPSEC tunnels, it is not supported for GRE tunnels. • **FEC Adaptive** – Corresponding packets are subjected to FEC only if the tunnels that they go through have been deemed unreliable based on measured loss. Adaptive FEC starts to work at 2% packet loss; this value is hard-coded and is not configurable. • **FEC Always** – Corresponding packets are always subjected to FEC. • **Packet Duplication** – Sends duplicate packets over a single tunnel. If more than one tunnel is available, duplicated packets will be sent over the tunnel with the best parameters.	**a.** In the **Match** conditions, click **Loss Correction**. **b.** In the **Loss Correction** field, select **FEC Adaptive**, **FEC Always**, or **Packet Duplication**.
Click **Save Match and Actions**.		

16. Create additional sequence rules as desired. Drag and drop to re-arrange them.

17. Click **Save Data Policy**.

18. Click **Next** to move to **Apply Policies to Sites and VPNs** in the wizard.

Apply Policies to Sites and VPNs

In the **Apply Policies to Sites and VPNs** screen, apply a policy to sites and VPNs:

1. In the **Policy Name** field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

2. In the **Policy Description** field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

3. Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:

   a. For a **Topology** policy block, click **New Site List**, **Inbound Site List**, **Outbound Site List**, or **VPN List**. Some topology blocks might have no **Add** buttons. Choose one or more site lists, and choose one or more VPN lists. Click **Add**.

b. For an **Application-Aware Routing** policy block, click **New Site List** and **VPN list**. Choose one or more site lists, and choose one or more VPN lists. Click **Add**.

c. For a **Traffic Data** policy block, click **New Site List and VPN List**. Choose the direction for applying the policy (**From Service**, **From Tunnel**, or **All**), choose one or more site lists, and choose one or more VPN lists. Click **Add**.

d. For a cflowd policy block, click **New Site List**. Choose one or more site lists, and click **Add**.

4. Click **Preview** to view the configured policy. The policy appears in CLI format.

5. Click **Save Policy**. The **Configuration** > **Policies** screen appears, and the policies table includes the newly created policy.

Activate a Centralized Policy

Activating a centralized policy sends that policy to all connected Cisco vSmart Controllers. To activate a centralized policy:

1. In Cisco vManage, select the **Configuration** > **Policies** screen. When you first open this screen, the **Centralized Policy** tab is selected by default.

2. Choose a policy.

3. Click the **More Actions** option to the right of the row, and click **Activate**. The **Activate Policy** popup appears. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy must be applied.

4. Click **Activate**.

Configure Centralized Policies Using the CLI

To configure a centralized control policy using the CLI:

1. Create a list of overlay network sites to which the centralized control policy is to be applied (in the **apply-policy** command):

```
vSmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id
```

The list can contain as many site IDs as necessary. Include one **site-id** command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–). Create additional site lists, as needed.

2. Create lists of IP prefixes, TLOCs, and VPNs as needed:

```
vSmart(config)# policy lists
vSmart(config-lists)# prefix-list list-name
vSmart(config-lists-list-name)# ip-prefix prefix/length
vSmart(config)# policy lists
vSmart(config-lists)# tloc-list list-name
vSmart(config-lists-list-name)# tloc address
color color
encap encapsulation
[preference value]
```

```
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-list-name)# vpn vpn-id
```

3. Create a control policy instance:

```
vSmart(config)# policy control-policy policy-name
vSmart(config-control-policy-policy-name)#
```

4. Create a series of match–action pair sequences:

```
vSmart(config-control-policy-policy-name)# sequence
number
vSmart(config-sequence-number)#
```

The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

5. Define match parameters for routes and for TLOCs:

```
vSmart(config-sequence-number)# match route route-parameter
vSmart(config-sequence-number)# match tloc tloc-parameter
```

6. Define actions to take when a match occurs:

```
vSmart(config-sequence-number)# action reject
vSmart(config-sequence-number)# action accept export-to (vpn
vpn-id | vpn-list list-name)
vSmart(config-sequence-number)# action accept set omp-tag
number

vSmart(config-sequence-number)# action accept set
preference value

vSmart(config-sequence-number)# action accept set
service service-name
(tloc ip-address |
tloc-list list-name)
[vpn vpn-id]

vSmart(config-sequence-number)# action accept set tloc
ip-address
color color
[encap encapsulation]
vSmart(config-sequence-number)# action accept set tloc-action
action

vSmart(config-sequence-number)# action accept set tloc-list list-name
```

7. Create additional numbered sequences of match–action pairs within the control policy, as needed.

8. If a route does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching routes to be accepted, configure the default action for the policy:

```
vSmart(config-policy-name)# default-action accept
```

9. Apply the policy to one or more sites in the Cisco SD-WAN overlay network:

```
vSmart(config)# apply-policy site-list
list-name
control-policy
policy-name (in | out)
```

10. If the action you are configuring is a service, configure the required services on the Cisco SD-WAN devices so that the Cisco vSmart Controller knows how to reach the services:

```
Device(config)# vpn vpn-id
service service-name
address ip-address
```

Specify the VPN is which the service is located and one to four IP addresses to reach the service device or devices. If multiple devices provide the same service, the device load-balances the traffic among them. Note that the Cisco SD-WAN device keeps track of the services, advertising them to the Cisco vSmart Controller only if the address (or one of the addresses) can be resolved locally, that is, at the device's local site, and not learned through OMP. If a previously advertised service becomes unavailable, the Cisco SD-WAN device withdraws the service advertisement.

Following are the high-level steps for configuring a VPN membership data policy:

1. Create a list of overlay network sites to which the VPN membership policy is to be applied (in the **apply-policy** command):

   ```
   vSmart(config)# policy
   vSmart (config-policy)# lists site-list list-name
   vSmart(config-lists-list-name)# site-id site-id
   ```

   The list can contain as many site IDs as necessary. Include one **site-id** command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–). Create additional site lists, as needed.

2. Create lists of IP prefixes and VPNs, as needed:

   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# data-prefix-list list-name
   vSmart(config-lists-list-name)# ip-prefix prefix/length
   ```

   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# vpn-list list-name
   vSmart(config-lists-list-name)# vpn vpn-id
   ```

3. Create lists of TLOCs, as needed.

   ```
   vSmart(config)# policy
   vSmart(config-policy)# lists tloc-list list-name
   vSmart(config-lists-list-name)# tloc ip-address color color encap encapsulation
   [preference number}
   ```

4. Define policing parameters, as needed:

   ```
   vSmart(config-policy)# policer policer-name
   vSmart(config-policer)# rate bandwidth
   vSmart(config-policer)# burst bytes
   vSmart(config-policer)# exceed action
   ```

5. Create a data policy instance and associate it with a list of VPNs:

   ```
   vSmart(config)# policy data-policy policy-name
   vSmart(config-data-policy-policy-name)# vpn-list list-name
   ```

6. Create a series of match–pair sequences:

   ```
   vSmart(config-vpn-list)# sequence number
   vSmart(config-sequence-number)#
   ```

   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

7. Define match parameters for packets:

```
vSmart(config-sequence-number)# match parameters
```

8. Define actions to take when a match occurs:

```
vSmart(config-sequence-number)# action (accept | drop) [count counter-name] [log]
[tcp-optimization]
vSmart(config-sequence-number)# action acccept nat [pool number] [use-vpn 0]
vSmart(config-sequence-number)# action accept redirect-dns (host | ip-address)
vSmart(config-sequence-number)# action accept set parameters
```

9. Create additional numbered sequences of match–action pairs within the data policy, as needed.

10. If a route does not match any of the conditions in one of the sequences, it is rejected by default. To accept nonmatching prefixed, configure the default action for the policy:

```
vSmart(config-policy-name)# default-action accept
```

11. Apply the policy to one or more sites in the overlay network:

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all
|from-service | from-tunnel)
```

Centralized Policies Configuration Examples

This topic provides some examples of configuring a centralized data policy to influence traffic flow across the Cisco SD-WAN domain and to configure a Cisco SD-WAN device to be an internet exit point.

General Centralized Policy Example

This section shows a general example of a centralized data policy to illustrate that you configure centralized data policy on a Cisco vSmart Controller and that after you commit the configuration, the policy itself is pushed to the required Cisco SD-WAN device.

Here we configure a simple data policy on the Cisco vSmart Controller vm9:

```
vm9# show running-config policy
policy
 data-policy test-data-policy
  vpn-list test-vpn-list
   sequence 10
    match
     destination-ip 209.165.201.0/27
    !
    action drop
     count test-counter
    !
   !
   default-action drop
  !
 !
 lists
  vpn-list test-vpn-list
   vpn 1
  !
  site-list test-site-list
   site-id 500
  !
 !
!
```

Immediately, after you activate the configuration on the Cisco vSmart Controller, it pushes the policy configuration to the Cisco vEdge devices in site 500. One of these devices is vm5, where you can see that the policy has been received:

```
vm5# show policy from-vsmart
policy-from-vsmart
 data-policy test-data-policy
  vpn-list test-vpn-list
   sequence 10
    match
     destination-ip 209.165.201.0/27
    !
    action drop
     count test-counter
    !
   !
   default-action drop
  !
 !
 lists
  vpn-list test-vpn-list
   vpn 1
  !
 !
!
```

Control Access

This example shows a data policy that limits the type of packets that a source can send to a specific destination. Here, the host at source address 192.0.2.1 in site 100 and VPN 100 can send only TCP traffic to the destination host at 203.0.113.1. This policy also specifies the next hop for the TCP traffic sent by 192.0.2.1, setting it to be TLOC 209.165.200.225, color gold. All other traffic is accepted as a result of the **default-action** statement.

```
policy
  lists
     site-list north
       site-id 100
     vpn-list vpn-north
       vpn 100
  !
  data-policy tcp-only
     vpn-list vpn-north
       sequence 10
         match
           source-ip 192.0.2.1/32
           destination-ip 198.51.100.1/32
           protocol tcp
         action accept
           set tloc 203.0.113.1 gold
       !
       default-action accept
   !
!
apply-policy
   site north data-policy tcp-only
```

Restrict Traffic

This examples illustrates how to disallow certain types of data traffic from being sent from between VPNs. This policy drops data traffic on port 25, which carries SMTP mail traffic, that originates in 209.165.201.0/27. However, the policy accepts all other data traffic, including non-SMTP traffic from 209.165.201.0/27.

```
policy
  lists
    data-prefix-list north-ones
      ip-prefix 209.165.201.0/27
      port 25
    vpn-list all-vpns
      vpn 1
      vpn 2
    site-list north
      site-id 100
  !
  data-policy no-mail
   vpn-list all-vpns
     sequence 10
       match
         source-data-prefix-list north-ones
       action drop
      !
     default-action accept
  !
!
apply-policy
  site north data-policy no-mail
```

Allow Traffic to Exit from a Cisco vEdge Device to the Internet

The following example allows data traffic destined for two prefixes on the Internet to exit directly from the local Cisco vEdge device to the internet destination. Configure this policy on the Cisco vSmart Controller.

```
polcy
 lists
  vpn-list vpn-1
    vpn 1
  !
  site-list nat-sites
    site-id 100,200
  !
data-policy accept-nat
  vpn-list vpn-1
   sequence 100
    match
     source-ip      10.20.24.0/24
     destination-ip 10.0.12.12/32
    !
    action accept
     count nat
     nat use-vpn 0
    !
   !
   sequence 101
    match
     source-ip      10.20.24.0/24
     destination-ip 10.1.15.13/32
    !
    action accept
     count nat_inet
     nat use-vpn 0
    !
   !
   default-action accept
  !
 !
apply-policy
  site-list nat-sites data-policy accept-nat
```

Using the destination port instead of a destination IP prefix allows greater flexibility for traffic exiting to the internet. Here, traffic can go to all HTTP and HTTPS sites (ports 80 and 443, respectively). Configure this policy on a Cisco vSmart Controller.

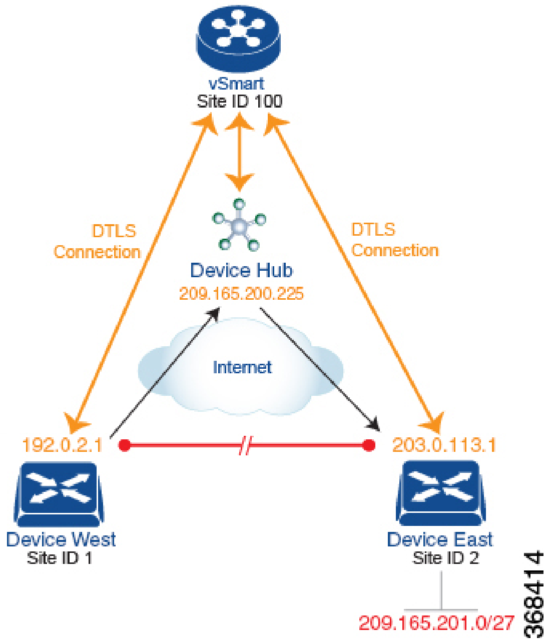
```
data-policy accept-nat
  vpn-list vpn-1
   sequence 100
    match
     source-ip      10.20.24.0/24
     destination-port 80
    !
    action accept
     count nat
     nat use-vpn 0
    !
   !
   sequence 101
    match
     source-ip      10.20.24.0/24
     destination-port 443
    !
    action accept
     count nat_inet
     nat use-vpn 0
    !
   !
   default-action accept
  !
 !
```

Traffic Engineering

This example of traffic engineering forces all traffic to come to a Cisco SD-WAN device using a device hub instead of directly.

One common way to design a domain in a Cisco SD-WAN overlay network is to route all traffic destined for branches through a hub router, which is typically located in a data center, rather than sending the traffic directly from one Cisco SD-WAN device to another. You can think of this as a hub-and-spoke design, where one device is acting as a hub and the devices are the spokes. With such a design, traffic between local branches travels over the IPsec connections that are established between the spoke routers and the hub routers when the devices are booted up. Using established connections means that the devices 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 devices, 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 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 the device spoke router traffic to a Cisco 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 devices in different branches:

- The Device West in site ID 1. The TLOC for this device is defined by its IP address (192.0.2.1), a color (gold), and an encapsulation (here, IPsec). We write the full TLOC address as {192.0.2.1, gold, ipsec}. The color is simply a way to identify a flow of traffic and to separate it from other flows.
- The Device East in site ID 2 has a TLOC address of {203.0.113.1, gold, ipsec}.

The devices West and East learn each other's TLOC addresses from the OMP routes distributed to them by the Cisco vSmart Controller. In this example, the Device East advertises the prefix 209.165.201.0/27 as being reachable at TLOC {203.0.113.1, gold, }. In the absence of any policy, the Device West could route traffic destined for 209.165.201.0/27 to TLOC {203.0.113.1, gold, ipsec}, which means that the Device West would be sending traffic directly to the Device East.

However, our design requires that all traffic from West to East be routed through the hub router, whose TLOC address is {209.165.200.225, gold, ipsec}, before going to the Device East. To effect this traffic flow, you define a policy that changes the route's TLOC. So, for the prefix 1209.165.201.0/27, you create a policy that changes the TLOC associated with the prefix 209.165.201.0/27 from {203.0.113.1, gold, ipsec}, which is the TLOC address of the Device East, to {209.165.200.225, gold, ipsec}, which is the TLOC address of the hub router. The result is that the OMP route for the prefix 209.165.201.0/27 that the Cisco vSmart Controller advertises to the Device West that contains the TLOC address of the hub router instead of the TLOC address of the Device East. From a traffic flow point of view, the Device West then sends all traffic destined for 209.165.201.0/27 to the hub router.

The device also learns the TLOC addresses of the West and East devices from the OMP routes advertised by the Cisco vSmart Controller. Because, devices must use these two TLOC addresses, no policy is required to control how the hub directs traffic to the devices.

Here is a policy configuration on the Cisco vSmart Controller that directs the Device West (and any other devices in the network domain) to send traffic destined to prefix 209.165.201.0/27 to TLOC 209.165.200.225, gold, which is the device:

```
policy
  lists
    prefix-list east-prefixes
      ip-prefix 209.165.201.0/27
    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 209.165.200.225 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 “209.165.201.0/27”
  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 “209.165.201.0/27”
      AND matches a route from site-id “2”
    If a match occurs:
      Accept the route
      AND change the route’s TLOC to “209.165.200.225” 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”, that is, to site ID 1
```

This control policy is configured on the Cisco vSmart Controller as an outbound policy, as indicated by the **out** option in the apply-policy site command. This option means the Cisco vSmart Controller applies the TLOC change to the OMP route after it distributes the route from its route table. The OMP route for prefix 209.165.201.0/27 that the Cisco vSmart Controller distributes to the Device West associates 209.165.201.0/27 with TLOC 209.165.200.225, gold. This is the OMP route that the Device West installs it in its route table. The end results are that when the Device West sends traffic to 209.165.201.0/27, the traffic is directed to the hub; and the Device West does not establish a DTLS tunnel directly with the Device East.

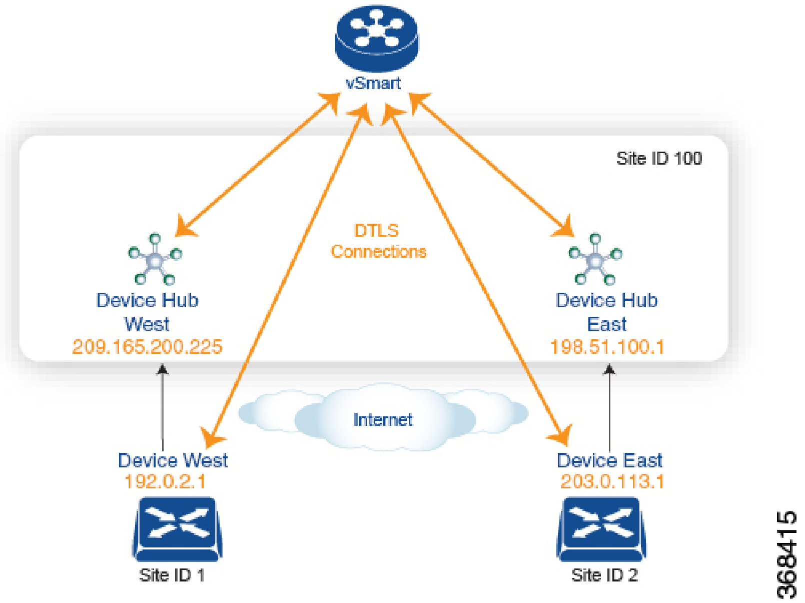
If the West side of the network had many sites instead of just one and each site had its own device, it would be straightforward to apply this same policy to all the sites. To do this, you simply add the site IDs of all the sites in the **site-list west-sites** list. This is the only change you need to make in the policy to have all the West-side sites send traffic bound for the prefix 209.165.201.0/27 through the device. For example:

```
policy
  lists
    prefix-list east-prefixes
      ip-prefix 209.165.201.0/27
    site-list west-sites
      site-id 1
      site-id 11
      site-id 12
      site-id 13
  control-policy change-tloc
    sequence 10
      match route
        prefix-list east-prefixes
        site-id 2
      action accept
        set tloc 209.165.200.225 color gold encap ipsec
apply-policy
  site west-sites control-policy change-tloc out
```

Creating Arbitrary Topologies

To provide redundancy in the hub-and-spoke-style topology discussed in the previous example, you can add a second Cisco hub to create a dual-homed hub site. The following figure shows that site ID 10 now has two Device hubs. We still want all inter-branch traffic to be routed through a device hub. However, because we now have dual-homed hubs, we want to share the data traffic between the two hub routers.

- Device Hub West, with TLOC 209.165.200.225, gold. We want all data traffic from branches on the West side of the overlay network to pass through and be processed by this device.
- Device Hub East, with TLOC 198.51.100.1, gold. Similarly, we all East-side data traffic to pass through the Device Hub East.



Here is a policy configuration on the Cisco vSmart Controller that would send West-side data traffic through the Cisco hub, and West and East-side traffic through the Device Hub East:

```
policy
  lists
    site-list west-sites
      site-id 1
    site-list east-sites
      site-id 2
    tloc-list west-hub-tlocs
      tloc-id 209.165.200.225 gold
    tloc-list east-hub-tlocs
      tloc-id 198.51.100.1 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 devices in the West portion of the overlay network.
- **site-list east-sites** lists the site IDs for the devices 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 Device West Hub, which we want to service traffic from the West-side device.
- **east-hub-tlocs** lists the TLOC for the Device East Hub, to service traffic from the East devices.

Define two control policies:

- **prefer-west-hub** affects OMP routes destined to TLOC 209.165.200.225, gold, which is the TLOC address of the Device West 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 Device West hub router.
- Similarly, **prefer-east-hub** sets the preference to 50 for OMP routes destined TLOC 198.51.100.1, gold, which is the TLOC address of the Device East hub router, thus directing traffic destined for site 100 site to the Device East hub 198.51.100.1 router.

Apply the control policies:

- The first line in the **apply-policy** configuration has the Cisco 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 routes destined to TLOC 209.165.200.225 is changed to 50 and traffic sent from the Device West to the hub site goes through the Device West hub router.
- The Cisco vSmart Controller applies the **prefer-east-hub** control policy to the OMP routes that it advertises to the devices in the **east-sites** list, which changes the preference to 50 for OMP routes destined to TLOC 198.51.100.1, so that traffic from the Device East goes to the Device East hub router.