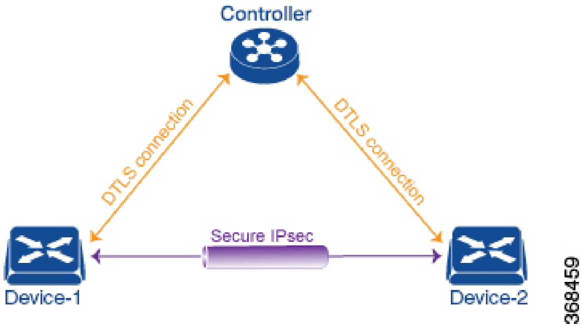
Data Policy

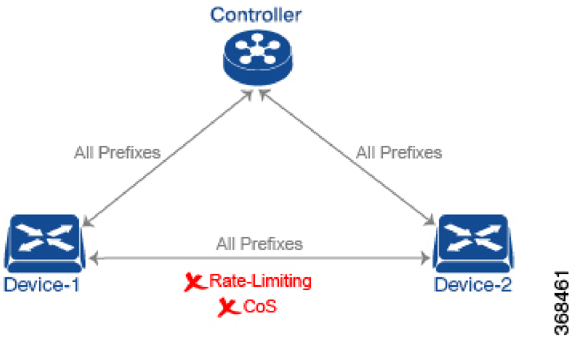
Data policy influences the flow of data traffic traversing the network based either on fields in the IP header of packets or the router interface on which the traffic is being transmitted or received. Data traffic travels over the IPsec connections between Cisco vEdge devices, shown in purple in the adjacent figure.



The Cisco Catalyst SD-WAN architecture implements two types of data policy:

- Centralized data policy controls the flow of data traffic based on the source and destination addresses and ports and DSCP fields in the packet's IP header (referred to as a 5-tuple), and based on network segmentation and VPN membership. These types of data policy are provisioned centrally, on the Cisco SD-WAN Controller, and they affect traffic flow across the entire network.
- Localized data policy controls the flow of data traffic into and out of interfaces and interface queues on a Cisco vEdge device. This type of data policy is provisioned locally using access lists. It allows you to classify traffic and map different classes to different queues. It also allows you to mirror traffic and to police the rate at which data traffic is transmitted and received.

By default, no centralized data policy is provisioned. The result is that all prefixes within a VPN are reachable from anywhere in the VPN. Provisioning centralized data policy allows you to apply a 6-tuple filter that controls access between sources and destinations.



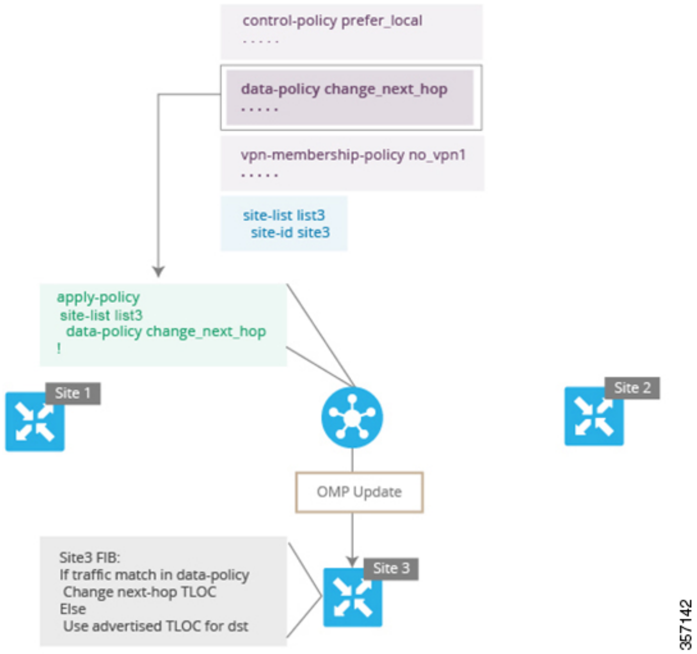
As with centralized control policy, you provision a centralized data policy on the Cisco SD-WAN Controller, and that configuration remains on the Cisco SD-WAN Controller. The effects of data policy are reflected in how the Cisco vEdge devices direct data traffic to its destination. Unlike control policy, however, centralized data polices are pushed to the devices in a read-only fashion. They are not added to the router's configuration file, but you can view them from the CLI on the router.

With no access lists provisioned on a Cisco vEdge device, all data traffic is transmitted at line rate and with equal importance, using one of the interface's queues. Using access lists, you can provision class of service, which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted. You can provision policing. You can also provision packet mirroring.

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 Cisco SD-WAN Controller, and then it is carried in OMP updates to the Cisco vEdge devices in the site-list that the policy is applied to. The match operation and any resultant actions are performed on the devices as it transmits or receives data traffic.

In the Data Policy Topology figure, a data policy named “change_next_hop” is applied to a list of sites that includes Site 3. The OMP update that the Cisco SD-WAN Controller sends to the devices at Site 3 includes this policy definition. When the device sends or receives data traffic that matches the policy, it changes the next hop to the specified TLOC. Non-matching traffic is forwarded to the original next-hop TLOC.

Figure 1: Data Policy Topology



```
control-policy prefer_local
.....
```

```
data-policy change_next_hop
.....
```

```
vpn-membership-policy no_vpn1
.....
```

```
site-list list3
  site-id site3
```

```
apply-policy
 site-list list3
  data-policy change_next_hop
!
```

```
Site3 FIB:
If traffic match in data-policy
 Change next-hop TLOC
Else
 Use advertised TLOC for dst
```

In the **apply-policy** command for a data policy, specify a direction from the perspective of the device. The "all" direction in the figure applies the policy to incoming and outgoing data traffic transiting the tunnel interface. 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.

- Centralized Policy, on page 3
- Localized Data Policy, on page 44

Centralized Policy

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

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 SD-WAN Manager or the CLI.

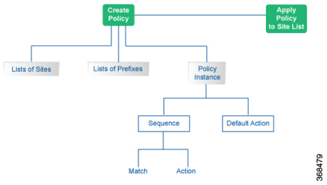
Configure Centralized Policy Based on Prefixes and IP Headers

A centralized data policy based on source and destination prefixes and on headers in IP packets consists of a series of numbered (ordered) sequences of match-action pair that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is dropped and discarded by default.

Configuration Components

The following figure illustrates the configuration components for a centralized data policy:



Start the Policy Configuration Wizard

To start the policy configuration wizard:

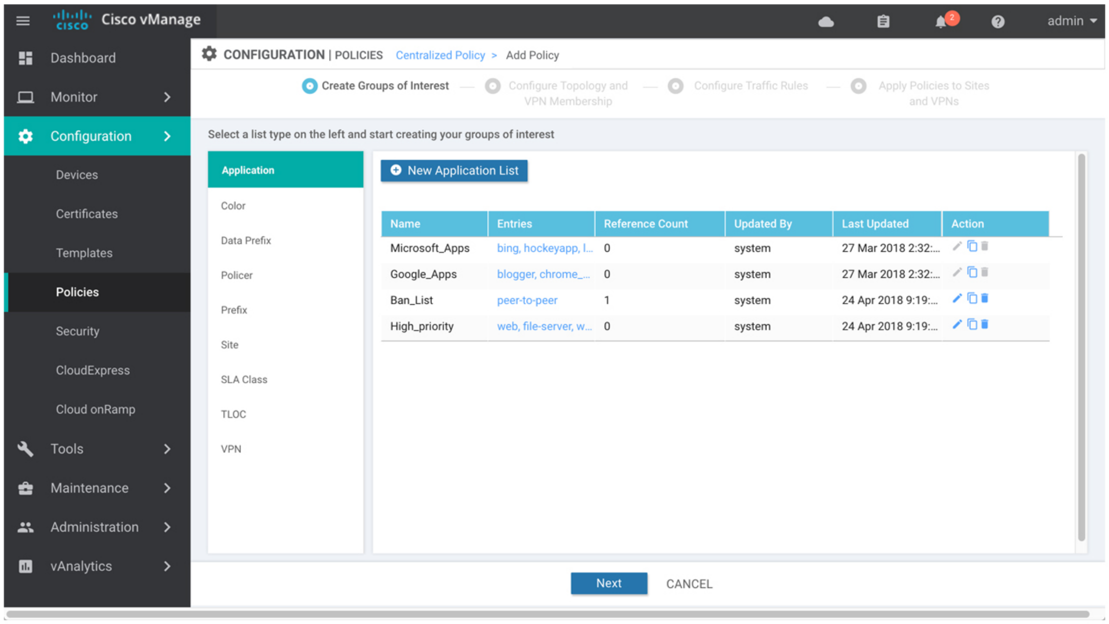
Step 1 In Cisco SD-WAN Manager, select the **Configuration** > **Policies** screen.

Step 2 Click**Centralized Policy**.

Step 3 Click **Add Policy**. The policy configuration wizard opens, and the Create Groups of Interest screen displays.

Step 1: Create Policy Lists

You can 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:...	

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

List Type	Procedure
Application	**a.** In the left bar, click **Application**. **b.** Click **New Application List**. **c.** Enter a name for the list. **d.** Choose either**Application**or **Application Family**. **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. • **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. • **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.

List Type	Procedure
Color	**a.** In the left bar, click **Color**. **b.** Click **New Color List**. The Color List popup displays. **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.** In the Add Data Prefix field, enter one or more data prefixes separated by commas. **e.** Click **Add**.
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**.

List Type	Procedure
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**.
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**.

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

Step 2: Configure Traffic Rules

Table 1: 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 Traffic Rules screen, the Application-Aware Routing tab is selected by default. To configure traffic rules for deep packet inspection, see Configure Deep Packet Inspection.

To configure traffic rules for centralized data policy:

Step 1 Click the **Traffic Data** tab.

Step 2 Click the **Add Policy** drop-down.

Step 3 Click **Create New**. The Add Data Policy screen displays.

Step 4 Enter a name and description for the data policy.

Step 5 In the right pane, click **Sequence Type**. The Add Data Policy popup opens.

Step 6 Select the type of data policy you want to create. Choices are: **Application Firewall**, **QoS**, **Service Chaining, Traffic Engineering**, and **Custom**.

Step 7 A policy sequence containing the text string **Application Firewall**, **QoS**, **Service Chaining, Traffic Engineering**, or **Custom** is added in the left pane

Step 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.

Step 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.

Step 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.

Step 11 To select one or more Match conditions, click its box and set the values as described in the following table. Note that not all match conditions are available for all policy sequence types.

Match Condition	Procedure	IPv4 Fields	IPv6 Fields
None (match all packets)	Do not specify any match conditions.	N/A	N/A

Match Condition	Procedure	IPv4 Fields	IPv6 Fields
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	N/A
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
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	N/A
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	N/A

Match Condition	Procedure	IPv4 Fields	IPv6 Fields
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.	N/A	N/A
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
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	N/A

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

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

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

Step 15 Set the policy action as described in the following table. Note that 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.
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**.		

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

Step 17 Click **Save Data Policy**.

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

Step 3: Apply Policies to Sites and VPNs

In Apply Policies to Sites and VPNs, apply a policy to overlay network sites and VPNs.

Step 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.

Step 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.

Step 3 From the Topology bar, select the tab that corresponds to the type of policy block—**Topology**, **Application-Aware Routing**, **Traffic Data**, or **Cflowd**. The table then lists policies that you have created for that type of policy block.

Step 4 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 **Add New Site List and VPN List** or **Add New Site**. Some topology blocks might have no **Add** buttons. Select one or more site lists, and select one or more VPN lists. Click **Add**.

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

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

d) For a **cflowd** policy block, click **Add New Site List**. Select one or more site lists. Click **Add**.

Step 5 Click **Preview** to view the configured policy. The policy is displayed in CLI format.

Step 6 Click **Save Policy**. The **Configuration** > **Policies** screen appears, and the policies table includes the newly created policy.

Step 4: Activate a Centralized Data Policy

Activating a centralized data policy sends that policy to all connected Cisco Catalyst SD-WAN Controllers. To activate a centralized policy:

Step 1 In Cisco SD-WAN Manager, select the **Configuration** > **Policies** screen.

Step 2 Select a policy from the policy table.

Step 3 Click the **More Actions** icon to the right of the row, and click **Activate**. The Activate Policy popup opens. It lists the IP addresses of the reachable Cisco Catalyst SD-WAN Controllers to which the policy is to be applied.

Step 4 Click **Activate**.

Configure Centralized Data Policy Using CLI

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)
```

Structural Components of Policy Configuration for Centralized Data Policy

The following commands are the structural components required to configure 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 2:

List Type	Description	Cisco SD-WAN Manager	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 SD-WAN Manager	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 SD-WAN Manager	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 highest preference value is used. If two or more of TLOCs have the highest 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 SD-WAN Manager 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 SD-WAN Manager, 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 - 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 SD-WAN Manager, 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 - Data Policy

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

Each sequence in a policy can contain one or more match conditions.

Table 3:

Match Condition	Description
Omit	Match all packets.
Applications/Application Family List	Applications or application families.

Match Condition	Description
Destination Data Prefix	Group of destination prefixes, IP prefix and prefix length. The range is 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 [-]).
Destination Region	Choose one of the following: • **Primary**: Match traffic if the destination device is in the same primary region (also called access region) as the source. This traffic reaches the destination using a multi-hop path, through the core region. • **Secondary**: Match traffic if the destination device is not in the same primary region as the source but is within the same secondary region as the source. This traffic can reach the destination using a direct tunnel, as described for secondary regions. • **Other**: Match traffic if the destination device is not in the same primary region or secondary region as the source. This traffic requires a multi-hop path from the source to the destination. **Note** Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a
DNS Application List	Enables split DNS, to resolve and process DNS requests and responses on an application-by-application basis. Name of an **app-list** list . This list specifies the applications whose DNS requests are processed.
DNS	Specify the direction in which to process DNS packets. 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	Specifies the DSCP value.
Packet length	Specifies the packet length. The range is 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)	Specifies the packet loss priority. 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.
Protocol	Specifies Internet protocol number. The range is 0 through 255.
ICMP Message	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.
Source Data Prefix	Specifies the group of source prefixes or an individual source prefix.
Source Port	Specifies the source port number. The range is 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	Specifies the TCP flag, syn.

Match Condition	Description
Traffic To	In a Multi-Region Fabric architecture, match border router traffic flowing to the access region that the border router is serving, the core region, or a service VPN. **Note** Minimum release: Cisco vManage Release 20.8.1

Note If IPv4 packet contains non-initial fragment of UDP or TCP datagram, it has no L4 ports information available because there is no UDP or TCP header. For such fragments destination-port or source-port match is ignored.

In the following example, all the UDP packets to destination port 161 and any other IPv4 packets having protocol ID field in IPv4 header set to 17 with IPv4 header having fragment-offset set will be dropped.

```
policy
 app-visibility
 access-list SDWAN_101
  sequence 100
   match
    destination-port 161
    protocol         17
   !
   action drop
   !
  !
```

Table 4: 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 5: 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

Action Parameters - Data Policy

Table 6: Feature History

Feature Name	Release Information	Description
Path Preference Support for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature extends to Cisco IOS XE Catalyst 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).
Next Hop Action Enhancement in Data Policies	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature enhances match action conditions in a centralized data policy for parity with the features configured on Cisco vEdge devices. When you are setting up next-hop-loose action, this feature helps to redirect application traffic to an available route when next-hop address is not available.

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

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:

Action Condition	Description
Click **Accept**	Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.
Cflowd	Enables cflowd traffic monitoring.
Counter	Counts the accepted or dropped packets. Specifies the name of a counter. Use the **show policy access-lists counters** command on the Cisco vEdge device.
Click **Drop**	Discards the packet. This is the default action.

Action Condition	Description
Log	Minimum release: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco vManage Release 20.11.1 Click **Log** to enable logging. When (DP, AAR or ACL) data policy packets are configured with log action, logs generated and logged to syslog. Due to the global **log-rate-limit**, not all logs are logged. 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. For information on **policy log-rate-limit** CLI, see **policy log-rate-limit** command in the Cisco Catalyst SD-WAN Qualified Command Reference Guide.
Redirect DNS	Redirects DNS requests to a particular DNS server. Redirecting requests is optional, but if you do so, you must specify both actions. 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. **Note** When you upgrade to releases later than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you must configure redirect DNS through **nat use-vpn 0** to redirect DNS to Direct Internet Interface (DIA). **Note** You can set only local TLOC preferences with redirect-dns as actions on the same sequence, but not remote TLOC. **Note** You cannot configure Redirect DNS and SIG at the same time. NAT DIA fallback and DNS redirection are not supported at the same time in data policy.
TCP Optimization	Fine-tune TCP to decrease round-trip latency and improve throughout for matching TCP traffic.
Secure Internet Gateway	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.

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

Action Condition	Description
Cflowd	Enables cflowd traffic monitoring.
NAT Pool or **NAT VPN**	Enables NAT functionality, so that traffic can be redirected directly to the internet or other external destination.
DSCP	DSCP value. The range is 0 through 63.
Forwarding Class	Name of the forwarding class.
Local TLOC	Enables sending packets to one of the TLOCs that matches the color and encapsulation. The available colors are: 3g, biz-internet, blue, bronze, custom1,custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red and silver. The encapsulation options are: **ipsec** and **gre**. 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. By default, encapsulation is **ipsec**.
Next Hop	Sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1, the **Use Default Route when Next Hop is not available** field is available next to the **Next Hop** action parameter. This option is available only when the sequence type is **Traffic Engineering** or **Custom**, and the protocol is either **IPv4** or **IPv6**, but not both.
Policer	Applies a policer. Specifies the name of policer configured with the **policy policer** command.
Service	Specifies 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. Standard services: **FW**, **IDS**, **IDP** Custom services: **netsvc1**, **netsvc2**,**netsvc3**, **netsvc4** TLOC list is configured with a **policy lists tloc-list** list. Configure the services themselves on the Cisco vEdge devices that are collocated with the service devices, using the **vpn service** command.

Action Condition	Description
TLOC	Direct traffic to a remote TLOC that 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 **VPN**.	Set the VPN that the packet is part of. The range is 0 through 65530.

Note Data policies are applicable on locally generated packets, including routing protocol packets, when the match conditions are generic.

Example configuration:

```
sequence 21
   match
    source-ip 10.0.0.0/8
   action accept
```

In such situations, it may be necessary to add a sequence in the data policy to escape the routing protocol packets. For example to skip OSPF, use the following configuration:

```
sequence 20
   match
    source-ip 10.0.0.0/8
    protocol  89
   action accept
sequence 21
   match
    source-ip 10.0.0.0/8
   action accept
```

The following table describes the IPv4 and IPv6 actions.

Table 7:

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 - 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 SD-WAN Manager, 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.

Apply Centralized Data Policy in the CLI

To apply a centralized data policy in the CLI:

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

By default, data policy applies to all data traffic passing through the device: the policy evaluates all data traffic going from the local site (that is, from the service side of the router) into the tunnel interface, and it evaluates all traffic entering to the local site through the tunnel interface. You can explicitly configure this behavior by including the **all** option. To have the data policy apply only to traffic coming from the service site and exiting from the local site through the tunnel interface, include the **from-service** option. To have the policy apply only to traffic entering from the tunnel interface and traveling to the service site, include the **from-tunnel** option. You can apply different data policies in each of the two traffic directions.

For all **data-policy** policies that you apply with **apply-policy** commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists **site-list 1 site-id 1-100** and **site-list 2 site-id 70-130**. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different **data-policy** policies, the attempt to commit the configuration on the Cisco Catalyst SD-WAN Controller would fail.

The same type of restriction also applies to the following types of policies:

- Application-aware routing policy (**app-route-policy**)
- Centralized control policy (**control-policy**)
- Centralized data policy used for cflowd flow monitoring (**data-policy** that includes a **cflowd** action and **apply-policy** that includes a **cflowd-template** command)

You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for **control-policy** and **data-policy** policies can have overlapping site IDs. So for the two example site lists above, **site-list 1 site-id 1-100** and **site-list 2 site-id 70-130**, you could apply one to a control policy and the other to a data policy.

As soon as you successfully activate the configuration by issuing a **commit** command, the Cisco Catalyst SD-WAN Controller pushes the data policy to the devices located in the specified sites. To view the policy as configured on the Cisco Catalyst SD-WAN Controllers, use the **show running-config** command on the Cisco Catalyst SD-WAN Controller:

```
vSmart# show running-config policy
vSmart# show running-config apply-policy
```

To view the policy that has been pushed to the Cisco vEdge device, use the **show policy from-vsmart** command on the Cisco vEdge device.

```
vEdge# show policy from-vsmart
```

Cisco Catalyst SD-WAN Application Intelligence Engine Flow Overview

The Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) flow provides the ability to look into the packet past the basic header information. The SAIE flow determines the contents of a particular packet, and then either records that information for statistical purposes or performs an action on the packet.

Note In Cisco vManage Release 20.7.1 and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

Benefits include increased visibility into the network traffic, which enables network operators to understand usage patterns and to correlate network performance information along with providing usage base billing or even acceptable usage monitoring. The SAIE flow can also reduce the overall costs on the network.

You can configure the SAIE flow using a centralized data policy. You define the applications of interest in a Cisco SD-WAN Manager policy list or with the **policy lists app-list** CLI command, and you call these lists in a **policy data-policy** command. You can control the path of the application traffic through the network by defining, in the **action** portion of the data policy, the local TLOC or the remote TLOC, or for strict control, you can define both.

The following list of protocols are not supported in SAIE flow:

- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)
- Internet Control Message Protocol (ICMP)
- Bidirectional Forwarding Detection (BFD)

Configure Cisco Catalyst SD-WAN Application Intelligence Engine Flow Using Cisco SD-WAN Manager

To configure the Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) flow, use the Cisco SD-WAN Manager policy configuration wizard. The wizard consists of the following sequential screens that guide you through the process of creating and editing policy components:

- Create Applications or Groups of Interest—Create lists that group together related items and that you call in the match or action components of a policy. For configuration details, see Configure Groups of Interest.
- Configure Traffic Rules—Create the match and action conditions of a policy. For configuration details, see Configure Traffic Rules.
- Apply Policies to Sites and VPNs—Associate policy with sites and VPNs in the overlay network.

Configure SD-WAN Application Intelligence Engine Flow Using the CLI

Following are the high-level steps for configuring a centralized data policy for the SD-WAN Application Intelligence Engine (SAIE) flow.

Note In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

1. Create a list of overlay network sites to which the data policy is to be applied using 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 applications and application families that are to be subject to the data policy. Each list can contain one or more application names, or one or more application families. A single list cannot contain both applications and application families.

```
vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-app-list)# app application-name

vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-applist)# app-family family-name
```

3. 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
```

4. 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]
```

5. 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
```

6. 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
```

7. 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).

8. Define match parameters based on applications:

   ```
   vSmart(config-sequence-number)# match app-list list-name
   ```

9. Define additional match parameters for data packets:

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

10. Define actions to take when a match occurs:

    ```
    vSmart(config-sequence-number)# action (accept | drop) [count]
    ```

11. For packets that are accepted, define the actions to take. To control the tunnel over which the packets travels, define the remote or local TLOC, or for strict control over the tunnel path, set both:

    ```
    vSmart(config-action)# set tloc ip-address color color encap encapsulation
    vSmart(config-action)# set tloc-list list-name
    vSmart(config-action)# set local-tloc color color encap encapsulation
    vSmart(config-action)# set local-tloc-list color color encap encapsulation [restrict]
    ```

12. Define additional actions to take.

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

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

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

15. 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)
    ```

```
vEdge(config)# policy app-visibility
```

Use the following show commands for visibility in to traffic classification:

- `show app dpi flows`
- `show support dpi flows active detail`
- `show app dpi application`
- `show support dpi flows expired detail`
- `show support dpi statistics`

Components of Policy Configuration for Deep Packet Inspection

Following are the components required to configure a centralized data policy for deep packet inspection. Each one is explained in more detail in the sections below.

```
On the vSmart controller:
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 bps
  data-policy policy-name
    vpn-list list-name
      sequence number
        match
          app-list list-name
          destination-data-prefix-list list-name
          destination-ip ip-addresses
          destination-port port-numbers
          dscp number
          packet-length number
          protocol protocol
          source-data-prefix-list list-name
          source-ip ip-addresses
          source-port port-numbers
          tcp flag
        action
          drop
          count counter-name
          log
          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)

On the vEdge router:
policy
  app-visibility
```

Action Parameters for Configuring SD-WAN Application Intelligence Engine Flow

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.

From the Cisco SD-WAN Manager menu, you can 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 under 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 8:

Description	Cisco SD-WAN Manager	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**	—
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 device.
Discard the packet. This is the default action.	Click **Drop**	**drop**	—
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.

To view the packet logs, use the **show app log flow** and **show log** commands.

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

Table 9:

Description	Cisco SD-WAN Manager	CLI Command	Value or Range
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 SD-WAN Manager	CLI Command	Value or Range
Direct matching packets to a TLOC that matches 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.
Direct matching packets to the name service, before delivering the traffic to its ultimate 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 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 is configured with a **policy lists tloc-list** list.
Direct matching packets to the named service that is reachable using a GRE tunnel whose source is in the transport VPN (VPN 0). If the GRE tunnel used to reach the service is down, packet routing falls back to using standard routing. To drop packets when a GRE tunnel to the service is unreachable, include the restrict option. In the service VPN, you must also advertise the service using the **service** command. You configure the GRE interface or interfaces in the transport VPN (VPN 0).	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**
Direct traffic to a remote TLOC. The TLOC is defined by its IP address, color, and encapsulation.	Click **Accept**, then action **TLOC**.	**set local-tloc color** *color* [**encap** *encapsulation*]	TLOC address, color, and encapsulation

Description	Cisco SD-WAN Manager	CLI Command	Value or Range
Direct traffic to one of the remote TLOCs in the TLOC list.	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

Default Action

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.

From the Cisco SD-WAN Manager menu, you modify the default action from **Configuration** > **Policies** > **Centralized Policy** > **Add Policy** > **Configure Traffic Rules** > **Application-Aware Routing** > **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.

Apply Centralized Policy for SD-WAN Application Intelligence Engine Flow

To ensure that a centralized data policy for the SD-WAN Application Intelligence Engine (SAIE) flow takes effect, you must apply it to a list of sites in the overlay network.

To apply a centralized policy in Cisco SD-WAN Manager, see *Configure Centralized Policy Using Cisco SD-WAN Manager*.

To apply a centralized policy in the CLI:

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

By default, data policy applies to all data traffic passing through the Cisco Catalyst SD-WAN Controller: the policy evaluates all data traffic going from the local site (that is, from the service side of the router) into the tunnel interface, and it evaluates all traffic entering to the local site through the tunnel interface. You can explicitly configure this behavior by including the **all** option. To have the data policy apply only to policy exiting from the local site, include the **from-service** option. To have the policy apply only to incoming traffic, include the **from-tunnel** option.

You cannot apply the same type of policy to site lists that contain overlapping site IDs. That is, all data policies cannot have overlapping site lists among themselves. If you accidentally misconfigure overlapping site lists, the attempt to commit the configuration on the Cisco Catalyst SD-WAN Controller fails.

As soon as you successfully activate the configuration by issuing a **commit** command, the Cisco Catalyst SD-WAN Controller pushes the data policy to the Cisco vEdge devices located in the specified sites. To view the policy as configured on the Cisco Catalyst SD-WAN Controller, use the **show running-config** command on the Cisco Catalyst SD-WAN Controller:

```
vSmart# show running-config policy
vSmart# show running-config apply-policy
```

To view the policy that has been pushed to the Cisco vEdge device, use the **show policy from-vsmart** command on the Cisco vEdge device.

```
vEdge# show policy from-vsmart
```

Centralized Policies Configuration Examples

This topic provides some examples of configuring a centralized data policy to influence traffic flow across the Cisco Catalyst SD-WAN domain and to configure a Cisco Catalyst 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 Catalyst SD-WAN Controller and that after you commit the configuration, the policy itself is pushed to the required Cisco Catalyst SD-WAN device.

Here we configure a simple data policy on the Cisco Catalyst SD-WAN 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 Catalyst SD-WAN 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 Catalyst SD-WAN 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 Catalyst SD-WAN 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
```

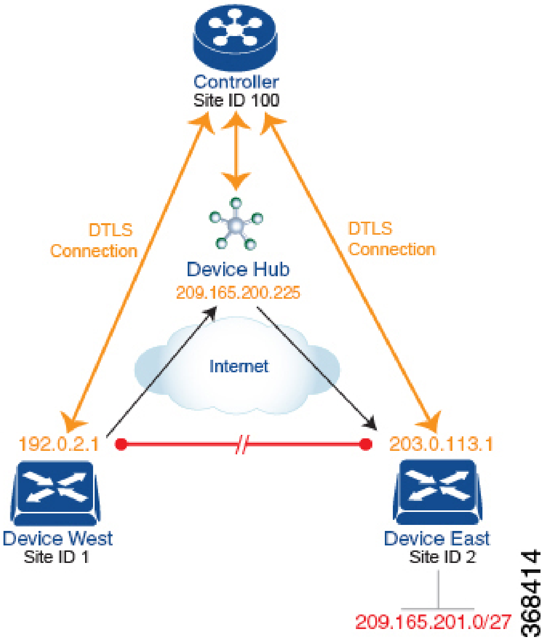
```
        count nat_inet
        nat use-vpn 0
      !
    !
    default-action accept
  !
!
```

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 Catalyst SD-WAN 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 209.165.201.0/27, 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 Catalyst SD-WAN 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 Catalyst SD-WAN 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 Catalyst SD-WAN 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 Catalyst SD-WAN Controller as an outbound policy, as indicated by the **out** option in the apply-policy site command. This option means the Cisco Catalyst SD-WAN 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 Catalyst SD-WAN 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.

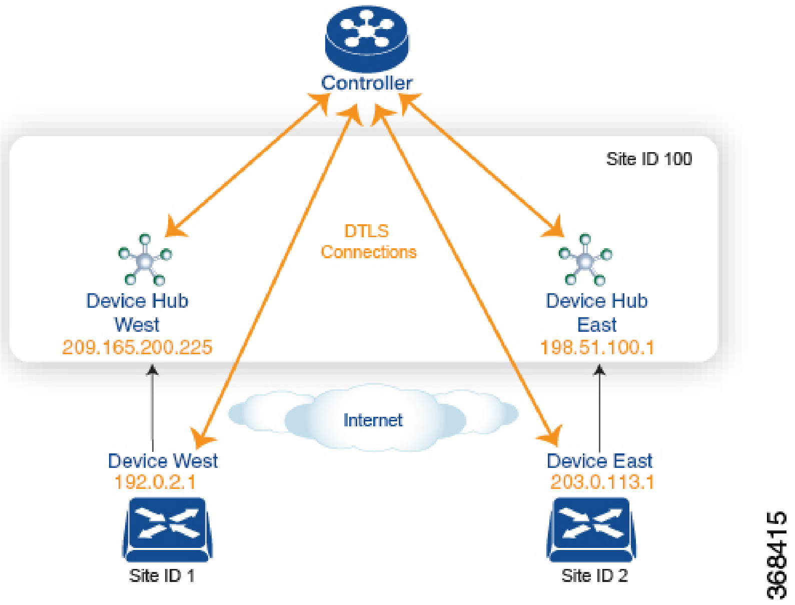
If the West side of the network had many sites instead of just one and each site had its own device, it would be straightforward to apply this same policy to all the sites. To do this, you simply add the site IDs of all the sites in the **site-list west-sites** list. This is the only change you need 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 100 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 Catalyst SD-WAN 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 Catalyst SD-WAN 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 Catalyst SD-WAN 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.

Localized Data Policy

Data policy operates on the data plane in the Cisco Catalyst SD-WAN overlay network and affects how data traffic is sent among the Cisco vEdge devices in the network. The Cisco Catalyst SD-WAN architecture defines two types of data policy, centralized data policy, which controls the flow of data traffic based on the IP header fields in the data packets and based on network segmentation, and localized data policy, which controls the flow of data traffic into and out of interfaces and interface queues on a Cisco vEdge device.

Localized data policy, so called because it is provisioned on the local Cisco vEdge device, is applied on a specific router interface and affects how a specific interface handles the data traffic that it is transmitting and receiving. Localized data policy is also referred to as access lists (ACLs). With access lists, you can provision class of service (CoS), classifying data packets and prioritizing the transmission properties for different classes. You can configure policing. You can also provision packet mirroring.

For IPv4, you can configure QoS actions.

You can apply IPv4 access lists in any VPN on the router, and you can create access lists that act on unicast and multicast traffic. You can apply IPv6 access lists only to tunnel interfaces in the transport VPN (VPN 0).

You can apply access lists either in the outbound or inbound direction on the interface. Applying an IPv4 ACL in the outbound direction affects data packets traveling from the local service-side network into the IPsec tunnel toward the remote service-side network. Applying an IPv4 ACL in the inbound direction affects data packets exiting from the IPsec tunnel and being received by the local Cisco vEdge device. For IPv6, an outbound ACL is applied to traffic being transmitted by the router, and an inbound ACL is applied to received traffic.

Explicit and Implicit Access Lists

Access lists that you configure using localized data policy are called *explicit* ACLs. You can apply explicit ACLs in any VPN on the router.

Router tunnel interfaces also have *implicit ACLs*, which are also referred to as *services*. Some of these are present by default on the tunnel interface, and they are in effect unless you disable them. Through configuration, you can also enable other implicit ACLs. On Cisco vEdge devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

Perform QoS Actions

With access lists, you can provision quality of service (QoS) which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted. See Forwarding and QoS Overview.

Mirror Data Packets

Once packets are classified, you can configure access lists to send a copy of data packets seen on a Cisco vEdge device to a specified destination on another network device. The Cisco vEdge devices support 1:1 mirroring; that is, a copy of every packet is sent to the alternate destination.

Localized Data Policy for IPv4

This topic provides procedures for configuring IPv4 localized data policy This type of data policy is called access lists, or ACLs. You can provision simple access lists that filter traffic based on IP header fields. You also use access lists to apply QoS, mirroring, and policing to data packets. You can create access lists that act on unicast and multicast traffic.

In Cisco SD-WAN Manager, you configure a localized data policy from the **Configuration** > **Policies** screen, using a policy configuration wizard. In the CLI, you configure these policies on the Cisco vEdge devices.

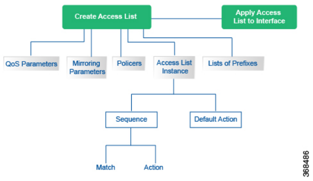
Configuration Components

An access list consists of a sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is, by default, dropped.

The following figure illustrates the configuration components for access lists.

Figure 2: Configuration Components



Configure Localized Data Policy for IPv4 Using Cisco SD-WAN Manager

Table 10: Feature History

Feature Name	Release Information	Description
Control Traffic Flow Using Class of Service Values	Cisco Catalyst SD-WAN Release 19.2.1	This feature lets you control the flow of traffic into and out of a Cisco Catalyst SD-WAN device interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule.

To configure IPv4 localized policy, use the Cisco SD-WAN Manager policy configuration wizard. The wizard is a UI policy builder that consists of five screens to configure IPv4 localized policy components:

- Groups of Interest, also called lists—Create data prefix lists and mirroring and policer parameters that group together related items and that you call in the match or action components of a policy.
- Forwarding Classes—Define forwarding classes and rewrite rules to use for QoS.
- Access Control Lists—Define the match and action conditions of ACLs.
- Route Policies—Define the match and action conditions of route policies.
- Policy Settings—Define additional policy settings, including Cloud QoS settings and the frequency for logging policy-related packet headers.

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the **Next** button at the bottom of the screen. To return to a component, click the **Back** button at the bottom of the screen.

Step 1: Start the Policy Configuration Wizard

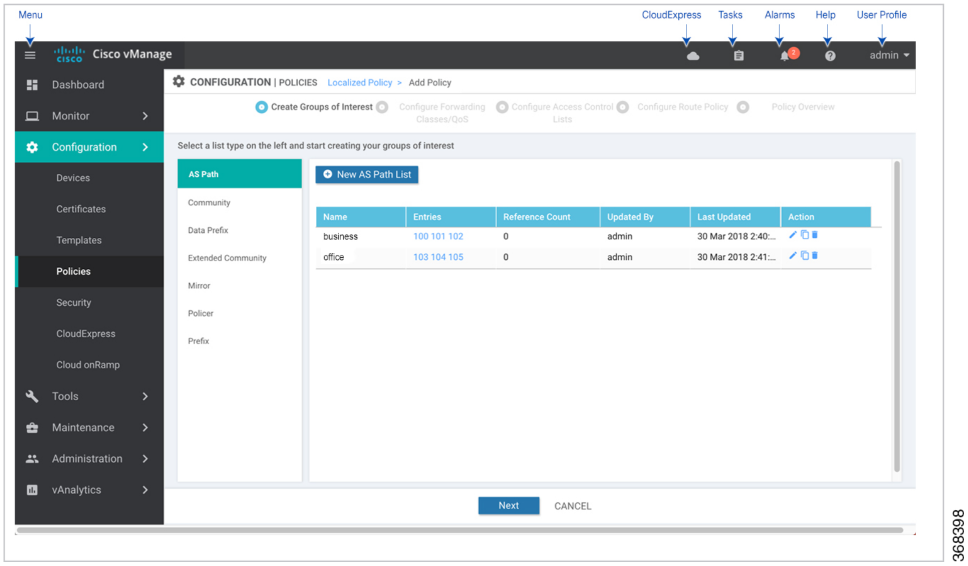
To start the policy configuration wizard:

1. In Cisco SD-WAN Manager, select the **Configuration** > **Policies** screen.
2. Select the **Localized Policy** tab.
3. Click **Add Policy**.

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

Step 2: Create Groups of Interest

In the Create Groups of interest screen, create lists to use in the localized data policy:



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

Name	Entries	Reference Count	Updated By	Last Updated	Action
business	100 101 102	0	admin	30 Mar 2018 2:40:...	
office	103 104 105	0	admin	30 Mar 2018 2:41:...	

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

List Type	Procedure
Data Prefix	a. In the left bar, click **Data Prefix**. b. Click **New Data Prefix List**. c. Enter a name for the list. d. Enter one or more IP prefixes. e. Click **Add**.
Mirror	a. In the left bar, click **Mirror**. b. Click **New Mirror List**. The Mirror List popup displays. c. Enter a name for the list. d. In the Remote Destination IP field, enter the IP address of the destination to which to mirror the packets. e. In the Source IP field, enter the IP address of the source of the packets to mirror. f. Click **Save**.

List Type	Procedure
Policer	**a.** In the left bar, click **Policer**. **b.** Click **New Policer List**. **c.** Enter a name for the list. **d.** In the Burst field, enter maximum traffic burst size. It can be a value from 15000 to 10000000 bytes. **e.** In the Exceed field, select the action to take when the burst size or traffic rate is exceeded. Select **Drop** (the default) to set the packet loss priority (PLP) to low. Select **Remark** to set the PLP to high. **f.** In the Rate field, enter the maximum traffic rate. It can be value from 0 through 2^{64} – 1 bps **g.** Click **Add**.

2. Click **Next** to move to Configure Forwarding Classes/QoS in the wizard.

Step 3: Configure Forwarding Classes for QoS

When you first open the Forwarding Classes/QoS screen, the **QoS** tab is selected by default:

To configure forwarding classes for use by QoS:

1. To create a new QoS mapping:
   a. In the QoS tab, click the **Add QoS** drop-down.
   b. Select **Create New**.
   c. Enter a name and description for the QoS mapping.
   d. Click **Add Queue**. The Add Queue popup displays.
   e. Select the queue number from the Queue drop-down.
   f. Select the maximum bandwidth and buffer percentages, and the scheduling and drop types. Enter the forwarding class.
   g. Click **Save**.

2. To import an existing QoS mapping:
   a. In the QoS tab, click the **Add QoS** drop-down.
   b. Select **Import Existing**.
   c. Select a QoS mapping.
   d. Click **Import**.

3. To view or copy a QoS mapping or to remove the mapping from the localized policy, click the **More Actions** icon to the right of the row, and select the desired action.

4. To configure policy rewrite rules for the QoS mapping:

   a. In the QoS tab, click the **Add Rewrite Policy** drop-down..

   b. Select **Create New**.

   c. Enter a name and description for the rewrite rule.

   d. Click **Add Rewrite Rule**. The Add Rule popup displays.

   e. Select a class from the Class drop-down.

   f. Select the priority (**Low** or **High**) from the Priority drop-down.

   g. Enter the DSCP value (0 through 63) in the DSCP field.

   h. Enter the class of service (CoS) value (0 through 7) in the Layer 2 Class of Service field.

   i. Click **Save**.

5. To import an existing rewrite rule:

   a. In the QoS tab, click the **Add Rewrite Policy** drop-down..

   b. Select **Import Existing**.

   c. Select a rewrite rule.

   d. Click **Import**.

6. Click **Next** to move to Configure Access Lists in the wizard.

Step 4: Configure ACLs

1. In the Configure Access Control Lists screen, configure ACLs.
2. To create a new IPv4 ACL, click the **Add Access Control List Policy** drop-down. Then select **Add IPv4 ACL Policy**.
3. Enter a name and description for the ACL.
4. In the left pane, click **Add ACL Sequence**. An Access Control List box is displayed in the left pane.
5. Double-click the **Access Control List** box, and type a name for the ACL.
6. In the right pane, click **Add Sequence Rule** to create a single sequence in the ACL. The Match tab is selected by default.
7. Click a match condition.
8. On the left, enter the values for the match condition.
9. On the right enter the action or actions to take if the policy matches.
10. Repeat Steps 6 through 8 to add match–action pairs to the ACL.
11. To rearrange match–action pairs in the ACL, in the right pane drag them to the desired position.
12. To remove a match–action pair from the ACL, click the **X** in the upper right of the condition.
13. Click **Save Match and Actions** to save a sequence rule.

14. To rearrange sequence rules in an ACL, in the left pane drag the rules to the desired position.
15. To copy, delete, or rename an ACL sequence rule, in the left pane, click **More Options** next to the rule's name and select the desired option.
16. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
    a. Click **Default Action** in the left pane.
    b. Click the **Pencil** icon.
    c. Change the default action to **Accept**.
    d. Click **Save Match and Actions**.
17. Click **Next** to move to Configure Route Policy in the wizard.
18. Click **Next** to move to the Policy Overview screen.

Step 5: Configure Policy Settings

In Policy Overview, configure policy settings:

1. Enter a name and description for the ACL.
2. To enable cflowd visibility so that a Cisco vEdge device can perform traffic flow monitoring on traffic coming to the device from the LAN, click **Netflow**.
3. To enable application visibility so that a Cisco vEdge device can monitor and track the applications running on the LAN, click **Application**.
4. To enable QoS scheduling and shaping for traffic that a Cisco vEdge device receives from transport-side interfaces, click **Cloud QoS**.
5. To enable QoS scheduling and shaping for traffic that a Cisco vEdge device receives from service-side interfaces, click **Cloud QoS Service Side**.
6. To log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface, click **Implicit ACL Logging**.
7. To configure how often packets flows are logged, click **Log Frequency**. Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.
8. Click **Preview** to view the full policy in CLI format.
9. Click **Save Policy**.

Step 6: Apply a Localized Data Policy in a Device Template

1. In Cisco SD-WAN Manager, select the **Configuration** > **Templates** screen.
2. If you are creating a new device template:
    a. In the Device tab, click **Create Template**.
    b. From the Create Template drop-down, select **From Feature Template**.
    c. From the Device Model drop-down, select one of the Cisco vEdge devices.

   d. In the Template Name field, enter a name for the device template. 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.

   e. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

   f. Continue with Step 4.

3. If you are editing an existing device template:

   a. In the Device tab, click the **More Actions** icon to the right of the desired template, and click the **Pencil** icon.

   b. Click the **Additional Templates** tab. The screen scrolls to the Additional Templates section.

   c. From the Policy drop-down, select the name of a policy that you have configured.

4. Click the **Additional Templates** tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Policy drop-down, select the name of the policy you configured in the above procedure.

6. Click **Create** (for a new template) or **Update** (for an existing template).

Components of Localized Policies

Components of Access Lists

Following are the structural components required to configure access lists.

```
policy
   implicit-acl-logging
   log-frequency number
   mirror mirror-name
      remote-dest ip-address source ip-address
   policer policer-name
      rate bandwidth
      burst bytes
      exceed action
policy ipv6
   access-list list-name
      sequence number
         match match-parameters
         action
            drop
            user counter-name
            log
            accept
               class class-name
               mirror mirror-name
               policer policer-name
     default-action (accept | drop)
vpn vpn-id
   interface interface-name
      ipv6 access-list list-name (in | out)
```

Lists

The localized policy uses the following types of lists to group related items. You configure lists under the **policy lists** command hierarchy on Cisco vEdge devices.

In Cisco SD-WAN Manager, you can configure lists from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Create Groups of Interest**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Lists** > **Data Prefix**

List Type	Description	CLI Command
AS paths	List of one or more BGP AS paths. You can write each AS as a single number or as a regular expression. To specify more than one AS in a single path, include the list in quotation marks (" "). To configure multiple AS paths in a single list, include multiple **as-path** options, specifying one AS path in each option.	**as-path-list** *list-name* **as-path** *path-list*
Communities	List of one or more communities. In **community**, you can specify: • *aa*:*nn*: Autonomous system number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS. • **no-advertise**: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.	**community-list** *list-name* **community** [*aa*:*nn* | **internet** | **local-as** | **no-advertise** | **no-export**]
Data prefixes	List of one or more IP prefixes. You can specify both unicast and multicast addresses. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.	**data-prefix-list** *list-name* **ip-prefix** *prefix/length*
Extended communities	List of one or more BGP extended communities. In **community**, you can specify: • **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the autonomous system number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the autonomous system number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.	**ext-community-list** *list-name* **community** [**rt** (*aa*:*nn* | *ip-address*) | **soo** (*aa*:*nn* | *ip-address*)]
Class Map	List of one or more classes.	**class** *class map*

List Type	Description	CLI Command
Mirror	List of one or more mirror parameters. To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets. Mirroring applies to unicast traffic only. It does not apply to multicast traffic.	**mirror** *mirror-name* **remote-dest** *ip-address* **source** *ip-address*
Policier	List of one or more policier parameters, such as burst, exceed, and rate. *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.	**policer** *policer-name* **rate** *bandwidth* **burst** *bytes* **exceed** *action*
Prefixes	List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. 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.	**prefix-list** *list-name* **ip-prefix** *prefix/length*

Logging Parameters

If you configure a logging action in a data policy, by default, the Cisco vEdge devices log all data packet headers to a syslog file. You can log only a sample of the data packet headers.

In Cisco SD-WAN Manager, you configure how often to log packet headers from:

Configuration > **Policies** > **Localized Policy** > **Add Policy** > **Policy Overview** > **Log Frequency field**

In the CLI, you configure this as follows:

```
vEdge(config)# policy log-frequency number
```

number specifies how often to to log packet headers. The default value is 1000. *number* can be an integer, and the software rounds the value down to the nearest power of 2. So for example, with the default value of 1000, the logging frequency is rounded down to 512, so every 512th packet is logged.

You can log the headers of all packets that are dropped because they do not match a service configured with an Allow Service configuration or an **allow-service** command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

In Cisco SD-WAN Manager, you configure this logging from:

Configuration > **Policies** > **Localized Policy** > **Add Policy** > **Policy Overview** > **Implicit ACL Logging field**

In the CLI, you do this as follows:

```
vEdge(config)# policy implicit-acl-logging
```

When you enable implicit ACL logging, by default, the headers of all dropped packets are logged. It is recommended that you configure a limit to the number of packets logged in the Log Frequency field or with the **log-frequency** command.

Mirroring Parameters

To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets.

In Cisco SD-WAN Manager, you configure mirroring parameters from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Create Groups of Interest** > **Mirror** > **New Mirror List**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Lists** > **Mirror** > **New Mirror List**

In the CLI, you configure mirroring parameters as follows:

```
vEdge(config)# policy mirror
mirror-namevEdge(config-mirror)# remote-dest ip-address
source
ip-address
```

Mirroring applies to unicast traffic only. It does not apply to multicast traffic.

QoS Parameters

In Cisco SD-WAN Manager, you can configure QoS parameters from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configuring Forwarding Classes/QoS**

  or

- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Configuring Forwarding Classes/QoS**

This section explains how to configure QoS parameters from the CLI.

To configure QoS parameters on a device, first define a classification. In Cisco SD-WAN Manager:

```
Device(config)# policy class-map class class-name queue number
```

class-name is the name of the class. It can be a text string from 1 through 32 characters long.

For hardware, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for low-latency queuing (LLQ), so any class that is mapped to queue 0 must be configured to use LLQ. The default scheduling method for all is weighted round-robin (WRR).

For Cisco vEdge devices, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for control traffic, and queues 1, 2, 3, 4, 5, 6 and 7 are available for data traffic. The scheduling method for all eight queues is WRR. LLQ is not supported.

To configure QoS parameters on a Cisco vEdge device, you must enable QoS scheduling and shaping. To enable QoS parameters for traffic that the Cisco vEdge device receives from transport-side interfaces:

```
Device(config)# policy cloud-qos
```

To enable QoS parameters for traffic that the Cisco vEdge device receives from service-side interfaces:

```
Device(config)# policy cloud-qos-service-side
```

Next, configure scheduling:

```
Device(config)# policy qos-scheduler scheduler-name
Device(config-qos-scheduler)# class percentage
Device(config-qos-scheduler)# buffer-percent percentage
Device(config-qos-scheduler)# drops (red-drop | tail-drop)
Device(config-qos-scheduler)# scheduling (llq | wrr)
```

scheduler-name is the name of the QoS scheduler. It can be a text string from 1 through 32 characters long.

class-name is the name of the forwarding class and can be a text string from 1 through 32 characters long. The common class names correspond to the per-hop behaviors AF (assured forwarding), BE (best effort), and EF (expedited forwarding).

The bandwidth percentage is the percentage of the interface's bandwidth to allocate to the forwarding class. The sum of the bandwidth on all forwarding classes on an interface should not exceed 100 percent.

The buffer percentage is the percentage of the interface's buffering capacity to allocate to the forwarding class. The sum of the buffering capacity of all forwarding classes on an interface should not exceed 100 percent.

Packets that exceed the bandwidth or buffer percentage are dropped either randomly, using random early detection (**red-drop**), or from the end of the queue (**tail-drop**). Low-latency queuing (LLQ) cannot use random early detection.

The algorithm to schedule interface queues can be either low-latency queuing (**llq**) or weighted round-robin (**wrr**).

Then, assign the scheduler to a QoS map:

```
Device(config-policy)# qos-map map-name qos-scheduler scheduler-name
```

map-name is the name of the QoS map, and *scheduler-name* is the name of the scheduler you configured above. Each name can be a text string from 1 through 32 characters long.

Finally, to configure a rewrite rule to overwrite the DSCP field of a packet's outer IP header:

```
Device(config)# policy rewrite-rule rule-name class class-name loss-priority
dscp dscp-value layer-2-cos number
```

rule-name is the name of the rewrite rule. It can be a text string from 1 through 32 characters long.

class-name is the name of a class you configured with the **qos-scheduler class** command. The packet loss priority (PLP) can be either **high** or **low**. To have a DSCP value overwrite the DSCP field of the packet's outer IP header, set a value from 0 through 63. To include an 802.1p marking in the packet, specify a number from 0 through 7.

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 SD-WAN Manager, 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

An access list contains sequences of match–action pairs. The sequences are numbered to set the order in which a packet is analyzed by the match–action pairs in the access lists.

In Cisco SD-WAN Manager, you configure sequences from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Add Access Control List Policy** > **Add ACL Sequence**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Access Control List Policy** > **Add Access Control List Policy** > **Add ACL Sequence**

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

Each sequence in an access list can contain one match condition and one action condition.

Match Parameters

Access List Parameters

Access lists can match IP prefixes and fields in the IP headers.

In the CLI, you configure the match parameters with the **policy access-list sequence match** command.

Each sequence in an access-list must contain one match condition.

Match class in ACL is not supported. You can use rewrite policy to configure DSCP values.

For access lists, you can match these parameters:

Match Condition	Description
Class	Name of a class defined with a **policy class-map** command.

Match Condition	Description
Destination Data Prefix	Name of a data-prefix-list list.
Destination Port	Specifies 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 [-]). The range is 0 through 65535.
DSCP	Specifies the DSCP value. The range is 0 through 63.
Protocol	Specifies the internet protocol number. The range is 0 through 255.
ICMP Message	When you select a Protocol value as 1 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. When you select a Next Header value as 58 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. **Note** This field is available from , Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1.
Packet Length	Specifies the length of the packet. The range can be from 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 [-]).
Source Data Prefix	Specifies the name of a **data-prefix-list** list.
PLP	Specifies the Packet Loss Priority (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.
Source Port	Specifies 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 [-]). The range is 0 through 65535.
TCP	**syn**

Route Policy Parameters

For route policies, you can match these parameters:

Match Condition	Description
Address	Specifies the name of a **Prefix-List** list.
AS Path List	Specifies one or more BGP AS path lists. You can write each AS as a single number or as a regular expression. To specify more than one AS number in a single path, include the list in quotation marks (" "). To configure multiple AS numbers in a single list, include multiple **AS Path** options, specifying one AS path in each option.

Match Condition	Description
Community List	List of one of more BGP communities. In **Community List**, you can specify: • *aa*:*nn*: AS number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS. • **no-advertise**: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.
Extended Community List	Specifies the list of one or more BGP extended communities. In **community**, you can specify: • **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.
BGP Local Preference	Specifies the BGP local preference number. The range is 0 through 4294967295.
Metric	Specifies the route metric value. The range is 0 through 4294967295.
Next Hop	Specifies the name of an IP prefix list.
OMP Tag	Specifies the OMP tag number. The range is 0 through 4294967295.
Origin	Specifies the BGP origin code. The optionss are: EGP (default), IGP, Incomplete.
OSPF Tag	Specifies the OSPF tag number. The range is 0 through 4294967295.
Peer	Specifies the peer IP address.

Action Parameters

Access List Parameters

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify, mirror, or police accepted packets.

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

Each sequence in an access list 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:

Action Condition	Description
Accept	Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the **action** portion of the access list.
Counter	Name of a counter. To display counter information, use the **show policy access-lists counters** command on the Cisco vEdge device.
Drop	Discards the packet. This is the default action.

For a packet that is accepted, the following actions can be configured:

Description	Value or Range
Class	Specifies the name of a QoS class. It can also be defined with a **policy class-map** command.
Mirror List	Specifies the name of mirror . It is defined with a **policy mirror** command.
Policer	Specifies the name of a policer defined with a **policy policer** command.
DSCP	Specifies the packet's DSCP value. The range is 0 through 63.
Next Hop	Specifies the IPv4 address. It sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco vManage Release 20.5.1 and Cisco SD-WAN Release 20.5.1, **Use Default Route when Next Hop is not available** field is available next to Next Hop action parameter.

Route Policy Parameters

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

When a route matches the conditions in the match portion of a route policy, the route can be accepted or rejected:

For a packet that is accepted, the following actions can be configured:

Description	Value or Range
Aggregator	Set sthe AS number in which a BGP route aggregator is located and the IP address of the route aggregator. The range is 1 through 65535.
As Path	Sets an AS number or a series of AS numbers to exclude from the AS path or to prepend to the AS path. The range is 1 through 65535.
Atomic Aggregate	Sets the BGP atomic aggregate attribute.
Community	Sets the BGP community value.
Local Preference	Sets the BGP local preference. The range is 0 through 4294967295.
Metric	Sets the metric value. The range is 0 through 4294967295.

Description	Value or Range
Metric Type	Sets the metric type. The options are type1 or type2.
Next Hop	Sets the IPv4 address. It sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco vManage Release 20.5.1 and Cisco SD-WAN Release 20.5.1, **Use Default Route when Next Hop is not available** field is available next to Next Hop action parameter.
OMP Tag	Sets the OMP tag for OSPF to use. The range is 0 through 4294967295.
Origin	Sets the BGP origin code. The options are: EGP (default), IGP, Incomplete.
Originator	Sets the IP address from which the route was learned.
OSPF Tag	Sets the OSPF tag value. The range is 0 through 4294967295.
Weight	Sets the BGP weight. The range is 0 through 4294967295.

Default Action

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

In Cisco SD-WAN Manager, you modify the default action from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Default Action**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Access Control List Policy** > **Default Action**

In the CLI, you modify this behavior with the **access-list default-action accept** command.

Apply Access Lists

For an access list to take effect, you must apply it to an interface.

In Cisco SD-WAN Manager, you apply the access list from **Configuration** > **Templates**. You can any of the interface feature configuration templates. For example, VPN interface cellular, ethernet, GRE, PPP and so on.

In the CLI, you apply the access list as follows:

```
Device(config)# vpn vpn-id interface interface-name
Device(config-interface)# access-list list-name (in|out)
```

Applying the policy in the inbound direction (**in**) affects prefixes being received on the interface. Applying it in the outbound direction (**out**) affects prefixes being transmitted on the interface.

For an access list that applies QoS classification, apply any DSCP rewrite rules to the same interface to which you apply the access list:

```
Device(config)# vpn vpn-id interface interface-name rewrite-rule rule-name
```

Note that you can also apply a policer directly to an interface, which has the effect of policing all packets transiting the interface, rather than policing only the selected packets that match the access list. You can apply the policer to either inbound or outbound packets:

```
Device(config)# vpn vpn-id interface interface-name
Device(config-interface)# policer
policer-name (in|out) interface-name
```

Explicit and Implicit Access Lists

Access lists that you configure through localized data policy using the **policy access-list** command are called *explicit* ACLs. You can apply explicit ACLs to any interface in any VPN on the device.

The device's tunnel interfaces in VPN 0 also have *implicit ACLs*, which are also referred to as *services*. Some services are enabled by default on the tunnel interface, and are in effect unless you disable them. Through configuration, you can also enable other services. You configure and modify implicit ACLs with the **allow-service** command:

```
Device(config)# vpn 0
Device(config-vpn)# interface interface-name
Device(config-interface)# tunnel-interface
Device(config-tunnel-interface)# allow-service service-name
Device(config-tunnel-interface)# no allow-service service-name
```

On Cisco vEdge devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. These three services allow the tunnel interface to accept DHCP, DNS, and ICMP packets. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

Note If a connection is initiated from a device, and if NAT is enabled on the device (for example, Direct Internet Access (DIA) is configured), return traffic is allowed by the NAT entry even if the implicit ACL has been configured as **no allow-service**. You can still block this traffic with an explicit ACL.

When data traffic matches both an explicit ACL and an implicit ACL, how the packets are handled depends on the ACL configuration. Specifically, it depends on:

- Whether the implicit ACL is configured as allow (**allow-service** *service-name*) or deny (**no allow-service** *service-name*). Allowing a service in an implicit ACL is the same as specifying the **accept** action in an explicit ACL, and a service that is not allowed in an implicit ACL is the same as specifying the **drop** action in an explicit ACL
- Whether, in an explicit ACL, the **accept** or **deny** action is configured in a policy sequence or in the default action.

The following table explains how traffic matching both an implicit and an explicit ACL is handled:

Table 11:

Implicit ACL	Explicit ACL: Sequence	Explicit ACL: Default	Result
Allow (accept)	Deny (drop)	—	Deny (drop)
Allow (accept)	—	Deny (drop)	Allow (accept)

Implicit ACL	Explicit ACL: Sequence	Explicit ACL: Default	Result
Deny (drop)	Allow (accept)	—	Allow (accept)
Deny (drop)	—	Allow (accept)	Deny (drop)

Configure Localized Policy for IPv4 Using the CLI

Following are the high-level steps for configuring an access list using the CLI for Cisco vEdge devices:

1. Create lists of IP prefixes as needed:

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

2. If you configure a logging action, configure how often to log packets to the syslog files:

   ```
   vEdge(config)# policy log-frequency number
   ```

3. For QoS, map each forwarding class to an output queue, configure a QoS scheduler for each forwarding class, and group the QoS schedulers into a QoS map:

   ```
   vEdge(config)# policy class-map
   vEdge(config-class-map)# class class-name queue number
   vEdge(config)# policy qos-scheduler scheduler-name
   vEdge(config-qos-scheduler)# class class-name
   vEdge(config-qos-scheduler)# bandwidth-percent percentage
   vEdge(config-qos-scheduler)# buffer-percent percentage
   vEdge(config-qos-scheduler)# drops drop-type
   vEdge(config-qos-scheduler)# scheduling type

   vEdge(config)# policy qos-map map-name qos-scheduler scheduler-name
   ```

4. For QoS, define rewrite rules to overwrite the DSCP field of a packet's outer IP header, if desired:

   ```
   vEdge(config)# policy rewrite-rule rule-name
   vEdge(config-rewrite-rule)# class class-name loss-priority
   dscp dscp-value layer-2-cos number
   ```

   class-name is one of the classes defined under a **qos-scheduler** command.

5. Define mirroring parameters (for unicast traffic only):

   ```
   vEdge(config)# policy mirror mirror-name
   vEdge(config-mirror)# remote-dest ip-address source ip-address
   ```

6. Define policing parameters:

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

7. Create an access list instance:

   ```
   vEdge(config)# policy access-list list-name
   ```

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

   ```
   vEdge(config-access-list)# sequence number
   vEdge(config-sequence)#
   ```

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).

9. Define match parameters for packets:

```
vEdge(config-sequence-number)
# match match-parameter
```

10. Define actions to take when a match occurs:

```
vEdge(config-sequence)# action drop
vEdge(config-sequence)# action count counter-name
vEdge(config-sequence)# action log
vEdge(config-sequence)# action accept class class-name
vEdge(config-sequence)# action accept mirror mirror-name
vEdge(config-sequence)# action accept policer policer-name
vEdge(config-sequence)# action accept set dscp value
vEdge(config-sequence)# action accept set next-hop ipv4-address
```

11. Create additional numbered sequences of match–action pairs within the access list, as needed.

12. If a packet does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching packets to be accepted, configure the default action for the access list:

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

13. Apply the access list to an interface:

```
vEdge(config)# vpn vpn-id interface interface-name
vEdge(config-interface)# access-list list-name (in | out)
```

Applying the access list in the inbound direction (**in**) affects packets being received on the interface. Applying it in the outbound direction (**out**) affects packets being transmitted on the interface. For QoS, apply a DSCP rewrite rule to the same egress interface:

```
vEdge(config)# vpn vpn-id interface interface-name rewrite-rule rule-name
```

14. You can apply a policer directly to an interface, which has the effect of policing all packets transiting the interface, rather than policing only the selected packets that match the access list. You can apply the policer to either inbound or outbound packets:

```
vEdge(config)# vpn vpn-id  interface interface-name
vEdge(config-interface)# policer policer-name (in | out)
```

Localized Data Policy for IPv6

This topic provides procedures for configuring IPv6 localized data policy This type of data policy is called access lists, or ACLs. You can provision simple access lists that filter traffic based on IP header fields. You also use access lists to apply mirroring and policing to data packets.

For IPv6, you can apply access lists only to interfaces in the transport VPN, VPN 0.

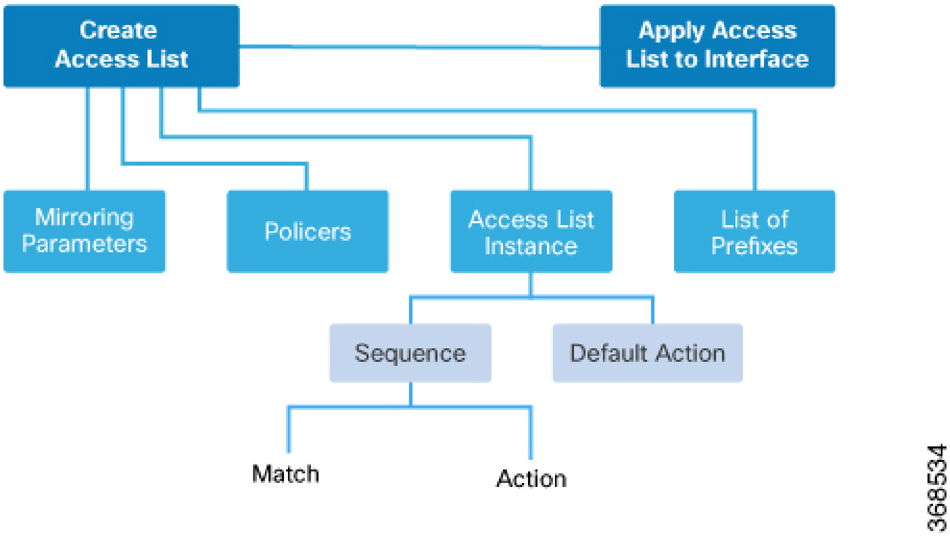
In Cisco SD-WAN Manager, you configure a localized data policy from the **Configuration** > **Policies** screen, using a policy configuration wizard. In the CLI, you configure these policies on the Cisco vEdge devices.

Configuration Components

An access list consists of a sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is, by default, dropped.

The following figure illustrates the configuration components for IPv6 access lists:



Configure Localized Data Policy for IPv6 Using vManage

To configure IPv6 localized data policy, use the Cisco SD-WAN Manager policy configuration wizard. The wizard is a UI policy builder that consists of five screens, and you use four of them to configure IPv6 localized policy components:

- Groups of Interest, also called *lists*—Create data prefix lists and mirroring and policer parameters that group together related items and that you call in the match or action components of a policy.
- Access Control Lists—Define the match and action conditions of ACLs.
- Route Policies—Define the match and action conditions of route policies.
- Policy Settings—Define additional policy settings. Specify the frequency for logging policy-related packet headers.

You configure some or all these components depending on the specific policy you are creating. To skip a component, click the **Next** button at the bottom of the screen. To return to a component, click the **Back** button at the bottom of the screen.

Step 1: Start the Policy Configuration Wizard

To start the policy configuration wizard:

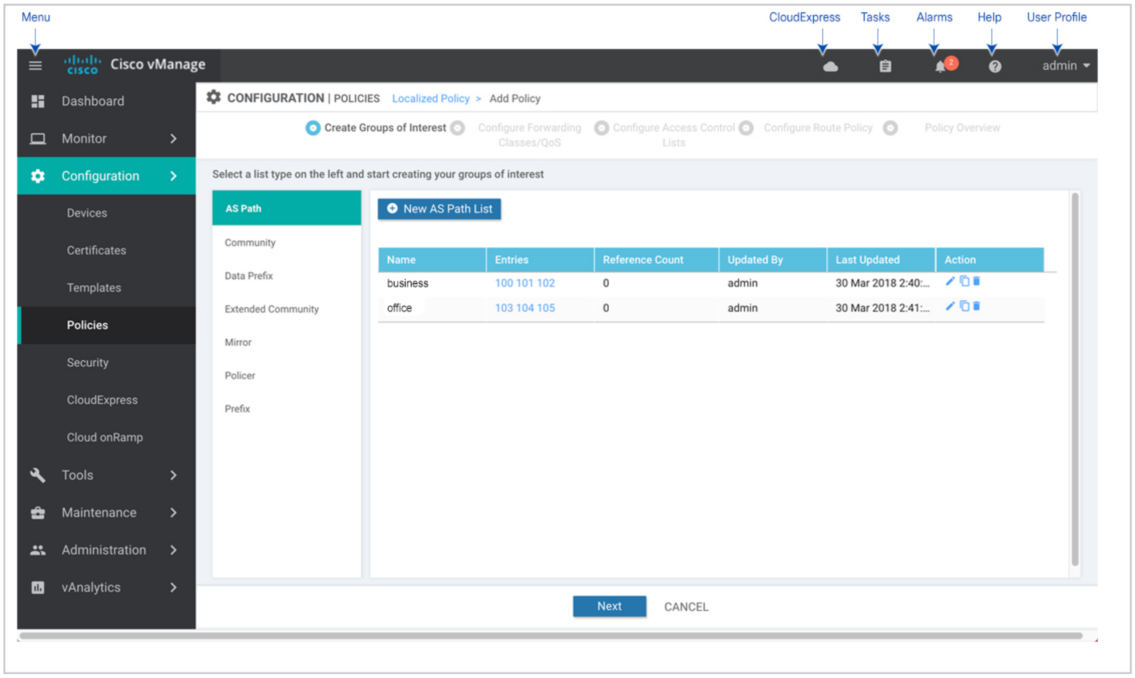
1. In Cisco SD-WAN Manager, select the **Configuration** > **Policies** screen. When you first open this screen, the Centralized Policy tab is selected by default.

2. Select the **Localized Policy** tab.

3. Click **Add Policy**. The policy configuration wizard opens, and the Create Groups of Interest screen is displayed.

Step 2: Create Groups of Interest

In the Create Groups of interest screen create lists to use in the localized data policy:



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

Name	Entries	Reference Count	Updated By	Last Updated	Action
business	100 101 102	0	admin	30 Mar 2018 2:40:...	
office	103 104 105	0	admin	30 Mar 2018 2:41:...	

368398

1. Create news lists of groups as described in the following table:

List Type	Procedure
AS Path	Permit or deny prefixes from certain autonomous systems. **a.** In the left bar, click **AS Path**. **b.** Enter a name for the list. For Cisco vEdge devices: Enter an alphanumeric value. **c.** Set the preference value for the list in the **Add AS Path** field.
Community	**a.** In the left bar, click **Community**. **b.** Click **New Community List**. **c.** Enter a name for the list. **d.** In the **Add Community** field, enter one or more data prefixes separated by commas. **e.** Click **Add**.

List Type	Procedure
Data Prefix	**a.** In the left bar, click **Data Prefix**. **b.** Click **New Data Prefix List**. **c.** Enter a name for the list. **d.** In the Internet Protocol field, click **IPv4** or **IPv6**. **e.** In the **Add Data prefix** field, enter one or more data prefixes separated by commas. **f.** Click **Add**.
Extended Community	**a.** In the left bar, click **Extended Community**. **b.** Click **New Extended Community List**. **c.** Enter a name for the list. **d.** In the **Add Extended Community** field, enter one or more data prefixes separated by commas. **e.** Click **Add**.
Class Map	Map a class name to an interface queue number. **a.** In the left bar, click **Class Map**. **b.** Click **New Class List**. The Class List popup displays. **c.** Enter a name for the list. The class name can be a text string from 1 to 32 characters long. **d.** Select a queue number between 0 and 7 from the **Queue** drop-down menu. **e.** Click **Save**.
Mirror	Define the remote destination for mirrored packets, and define the source of the packets. **a.** In the left bar, click **Mirror**. **b.** Click **New Mirror List**. **c.** Enter a name for the list. **d.** Enter the **Remote Destination IP** address in the left field, where the mirrored traffic should be routed. **e.** Enter the **Source IP** address of the mirrored traffic in the right field. **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, or **remark**, which sets the PLP to high. **3.** In the **Rate** field, enter the maximum traffic rate, a value from 0 through 264 – 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.** Click either **IPv4** or **IPv6**. **e.** Under **Add Prefix**, enter the prefix for the list. (An example is displayed.) Optionally, click the green **Import** link on the right-hand side to import a prefix list. **f.** Click **Add**.

2. Click **Next** to move to Configure Forwarding Classes/QoS in the wizard. For IPv6 localized data policy, you cannot configure QoS.

3. Click **Next** to move to Configure Access Lists in the wizard.

Step 3: Configure ACLs

1. In the Configure Access Control Lists screen, click **Add Access Control List Policy**, and choose **Add IPv6 ACL Policy** from the drop-down.

2. Enter a name and description for the ACL.

3. From the left column, click **Add ACL Sequence**.

4. Click **Sequence Rule** to open the ACL match/action sequence menu.

5. Click a match condition. See Match Parameters for a full description of these options.

6. On the left side, enter the values for the match condition.

7. On the right side, enter the action or actions to take if the policy matches. See Action Parameters for a full description of these options.
8. Repeat Steps 3 through 7 to add match–action pairs to the ACL.
9. To rearrange match–action pairs in the ACL, drag them to the desired position in the right pane.
10. To remove a match–action pair from the ACL, click the X in the upper right of the condition.
11. Click **Save Match and Actions** to save a sequence rule.
12. To copy, delete, or rename an ACL sequence rule, in the left pane, click the **More Options** menu (three dots) next to the rule's name and select the desired option.
13. If no packets match any of the ACL sequence rules, the default action is to drop the packets. To change the default action:
    a. Click **Default Action** in the left pane.
    b. Click the Pencil icon.
    c. Change the default action to **Accept.**
    d. Click **Save Match and Actions**.
14. Click **Next** to move to Configure Route Policy in the wizard.
15. Click **Next** to move to the Policy Overview screen.

Step 4: Configure Policy Settings

In Policy Overview, configure policy settings:

1. Enter a name and description for the ACL.
2. Under **Policy Settings**, select one of the following policy options:

Policy Settings Options	Description
Netflow	
Application	
Cloud QoS	
Cloud QoS Service side	
Implicit ACL Logging	Log the headers of all packets that are dropped because they do not match a service configured by an Allow Service parameter on a tunnel interface.
Log Frequency	Configure how often packet flows are logged. Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.

3. Click **Preview** to view the full policy in CLI format.

4. Click **Save Policy**.

Step 5: Apply a Localized Data Policy in a Device Template

1. In Cisco SD-WAN Manager, select the **Configuration** > **Templates** screen.
2. If you are creating a new device template:
   a. In the Device tab, click **Create Template**.
   b. From the Create Template drop-down, select **From Feature Template**.
   c. From the **Device Model** drop-down, select a Cisco vEdge device.
   d. In the **Template Name** field, enter a name for the device template. 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.
   e. In the **Description** field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
   f. Continue with Step 4.
3. If you are editing an existing device template:
   a. In the **Device** tab, click the **More Actions** icon to the right of the desired template, and click the pencil icon.
   b. Click the **Additional Templates** tab. The screen scrolls to the Additional Templates section.
   c. From the Policy drop-down, select the name of a policy that you have configured.
4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the Additional Templates section.
5. From the Policy drop-down, select the name of the policy you configured in the above procedure.
6. Click **Create** (for a new template) or **Update** (for an existing template).

Structural Components of Configuration for Access Lists

Following are the structural components required to configure access lists. Each one is explained in more detail in the sections below.

```
policy
   implicit-acl-logging
   log-frequency number
   mirror mirror-name
      remote-dest ip-address source ip-address
   policer policer-name
      rate bandwidth
      burst bytes
      exceed action
policy ipv6
   access-list list-name
      sequence number
         match match-parameters
```

```
            action
              drop
              user counter-name
              log
              accept
                class class-name
                mirror mirror-name
                policer policer-name
        default-action (accept | drop)
vpn vpn-id
  interface interface-name
    ipv6 access-list list-name (in | out)
```

Logging Parameters

If you configure a logging action in a data policy, by default, the Cisco vEdge device logs all data packet headers to a syslog file. You can log only a sample of the data packet headers.

In Cisco SD-WAN Manager, you configure how often to log packet headers from **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Policy Overview** > **Log Frequency** field.

In the CLI, you configure this as follows:

```
vEdge(config)# policy implicit-acl-logging
```

You can log the headers of all packets that are dropped because they do not match a service configured with an Allow Service configuration or an **allow-service** command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

In Cisco SD-WAN Manager, you configure this logging from the **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Policy Overview** > **Implicit ACL Logging** field.

In the CLI, you do this as follows:

```
vEdge(config)# policy implicit-acl-logging
```

When you enable implicit ACL logging, by default, the headers of all dropped packets are logged. It is recommended that you configure a limit to the number of packets logged in the Log Frequency field or with the **log-frequency** command.

Mirroring Parameters

To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets.

In Cisco SD-WAN Manager, you configure mirroring parameters from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Create Groups of Interest** > **Mirror** > **New Mirror List**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Lists** > **Mirror** > **New Mirror List**

In the CLI, you configure mirroring parameters as follows:

```
device(config)# policy mirror mirror-name
device(config-mirror)# remote-dest ip-address source ip-address
```

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 SD-WAN Manager, you configure policer parameters from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Create Groups of Interest** > **Policer** > **New Policer List**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Lists** > **Policer** > **New Policer List**

In the CLI, you configure policer parameters as follows:

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

- **`rate`** is the maximum traffic rate. It can be a value from 0 through $2^{64} - 1$ 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

Sequences

An access list contains sequences of match–action pairs. The sequences are numbered to set the order in which a packet is analyzed by the match–action pairs in the access lists.

In Cisco SD-WAN Manager, you configure sequences from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Add Access Control List Policy** > **Add ACL Sequence**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > > **Access Control List Policy** > **Add Access Control List Policy** > **Add ACL Sequence**

In the CLI, you configure sequences with the **policy ipv6 access-list sequence** command.

Each sequence in an access list can contain one match condition and one action condition.

Match Parameters

Access lists can match IP prefixes and fields in the IP headers.

In Cisco SD-WAN Manager, you configure match parameters from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Add Access Control List Policy** > **Add ACL Sequence** > **Add Sequence Rule** > > **Match**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Access Control List Policy** > **Add Access Control List Policy** > **Add ACL Sequence** > **Add Sequence Rule** > > **Match**

In the CLI, you configure the match parameters with the **policy ipv6 access-list sequence match** command.

Each sequence in an access list must contain one match condition.

For access lists, you can match these parameters:

Description	Cisco SD-WAN Manager	CLI Command	Value or Range
Enter a Destination port number.	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 [-])
Select the Next Header protocol	Next Header	**next-header** *number*	0 through 255, corresponding to an https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
Specify the packet length	Packet Length	**packet-length** *number*	Length of the packet. *number* can be from 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 [-])
Specify the packet loss priority (PLP)	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.
Select a Source data prefix list	N/A	N/A	
Enter a Source port number	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 [-])
Enter a Destination Data Prefix	N/A	N/A	
TCP	TCP	**tcp** *flag*	**syn**
Set the packet's DSCP value	Class	**set class** *value*	0 through 63
Traffic class	Traffic Class	**traffic-class** *value*	0 through 63

Action Parameters

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify, mirror, or police accepted packets.

In Cisco SD-WAN Manager, you configure match parameters from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Add Access Control List Policy** > **Add ACL Sequence** > **Add Sequence Rule** > **Action**
- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Access Control List Policy** > **Add Access Control List Policy** > **Add ACL Sequence** > **Add Sequence Rule** > **Action**

In the CLI, you configure the actions parameters with the **policy ipv6 access-list sequence action** command.

Each sequence in an access list 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:

For a packet that is accepted, the following actions can be configured:

Description	Cisco SD-WAN Manager	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 access list.	Click **Accept.**	`accept`	—
Count the accepted or dropped packets.	**Counter Name**	`count` *counter-name*	Name of a counter. To display counter information, use the **show ipv6 policy access-lists counters** command on the Cisco vEdge device.
Log the packet headers 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.	**Log**	`log`	To display logging information, use the **show app log flow-all** and **show app log flows** command on the Cisco vEdge device.
Designate the next hop router.	**Next Hop**	N/A	
Traffic Class	N/A	**set traffic-class** *value*	0-63
Mirror the packet.	Mirror List	**mirror** *mirror-name*	Name of mirror defined with a **policy mirror** command.
Set the packet's DSCP value.	Class	N/A	0 through 63
Police the packet.	Policer	**policer** *policer-name*	Name of a policer defined with a **policy policer** command.
Discard the packet. This is the default action.	Click **Drop**.	**drop**	—

Default Action

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

In Cisco SD-WAN Manager, you modify the default action from:

- **Configuration** > **Policies** > **Localized Policy** > **Add Policy** > **Configure Access Control Lists** > **Default Action**

- **Configuration** > **Policies** > **Custom Options** > **Localized Policy** > **Access Control List Policy** > **Default Action**

In the CLI, you modify this behavior with the **access-list ipv6 default-action accept** command.

Apply Access Lists

For an access list to take effect, you must apply it to a tunnel interface in VPN 0.

In Cisco SD-WAN Manager, you apply the access list in one of the interface feature configuration templates.

In the CLI, you apply the access list as follows:

```
vEdge(config)# vpn 0 interface  interface-name
vEdge(config-interface)# ipv6 access-list list-name (in | out)
```

Applying the policy in the inbound direction (`in`) affects prefixes being received on the interface. Applying it in the outbound direction (`out`) affects prefixes being transmitted on the interface.

Explicit and Implicit Access Lists

Access lists that you configure through localized data policy using the **policy access-list** command are called *explicit* ACLs. You can apply explicit ACLs to any interface in any VPN on the router.

The router's tunnel interfaces in VPN 0 also have implicit ACLs, which are also referred to as *services*. Some services are enabled by default on the tunnel interface, and are in effect unless you disable them. Through configuration, you can also enable other services. You configure and modify implicit ACLs with the **allow-service** command:

```
Device(config)# vpn 0
Device(config-vpn)# interface interface-name
Device(config-interface)# tunnel-interface
Device(config-tunnel-interface)# allow-service service-name
Device(config-tunnel-interface)# no allow-service service-name
```

On Cisco Catalyst SD-WAN devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. These three services allow the tunnel interface to accept DHCP, DNS, and ICMP packets. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

Note If a connection is initiated from a device, and if NAT is enabled on the device (for example, Direct Internet Access (DIA) is configured), return traffic is allowed by the NAT entry even if the implicit ACL has been configured as **no allow-service**. You can still block this traffic with an explicit ACL.

When data traffic matches both an explicit ACL and an implicit ACL, how the packets are handled depends on the ACL configuration. Specifically, it depends on:

- Whether the implicit ACL is configured as allow (**`allow-service`** *service-name*) or deny (**`no allow-service`** *service-name*). Allowing a service in an implicit ACL is the same as specifying the **`accept`** action in an explicit ACL, and a service that is not allowed in an implicit ACL is the same as specifying the **`drop`** action in an explicit ACL.

- Whether, in an explicit ACL, the **`accept`** or **`deny`** action is configured in a policy sequence or in the default action.

The following table explains how traffic matching both for an implicit and an explicit ACL is handled:

Implicit ACL	Explicit ACL: Sequence	Explicit ACL: Default	Result
Allow (accept)	Deny (drop)	—	Deny (drop)
Allow (accept)	—	Deny (drop)	Allow (accept)
Deny (drop)	Allow (accept)	—	Allow (accept)
Deny (drop)	—	Allow (accept)	Deny (drop)

Configure Localized Policy for IPv6 Using the CLI

Following are the high-level steps for configuring an access list using the CLI:

1. Define mirroring parameters (for unicast traffic only):

```
vEdge(config)# policy mirror mirror-name
vEdge(config-mirror)# remote-dest ip-address source ip-address
```

2. Define policing parameters:

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

3. Create an access list instance:

```
vEdge(config)# policy ipv6 access-list list-name
```

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

```
vEdge(config-ipv6-access-list)# sequence number
vEdge(config-sequence)#
```

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 packets:

```
vEdge(config-sequence-number)# match match-parameter
```

6. Define actions to take when a match occurs:

```
vEdge(config-sequence)# action drop
vEdge(config-sequence)# action count counter-name
vEdge(config-sequence)# action log
vEdge(config-sequence)# action accept class class-name
vEdge(config-sequence)# action accept mirror mirror-name
vEdge(config-sequence)# action accept policer policer-name
```

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

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

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

9. Apply the access list to an interface:

```
vEdge(config)# vpn vpn-id interface interface-name
vEdge(config-interface)# ipv6 access-list list-name (in | out)
```

Applying the access list in the inbound direction (**in**) affects packets being received on the interface. Applying it in the outbound direction (**out**) affects packets being transmitted on the interface.

Localized Data Policy Configuration Examples

This topic provides some straightforward examples of configuring localized data policy to help you get an idea of how to use policy to influence traffic flow across the Cisco Catalyst SD-WAN domain. Localized data policy, also known as access lists, is configured directly on the local Cisco vEdge devices.

QoS

You can configure quality of service (QoS) to classify data packets and control how traffic flows out of and in to the interfaces on a Cisco vEdge device and on the interface queues. For examples of how to configure a QoS policy, see Forwarding and QoS Configuration Examples.

Mirroring Example

This example illustrates how to configure a mirror instance to automatically send a copy of certain types of data packet to a specified destination for analysis. After you configure the mirror instance, include it in an access list. Here, "mirror-m1" is configured with the host at source address 10.20.23.16 and destination host at 10.2.2.11. The mirror instance is then included in the access list "acl2," which is configured so that data packets originating from the host at source address 10.20.24.17 and going to the destination host at 10.20.25.18 are mirrored to the destination host at 10.2.2.11 with the source address of the originating host as 10.20.23.16.

```
policy
 mirror m1
  remote-dest 10.2.2.11 source 10.20.23.16
 !
!

vm5# show running-config policy access-list acl2
policy
 access-list acl2
  sequence 1
   match
    source-ip      10.20.24.17/32
    destination-ip 10.20.25.18/32
   !
   action accept
    mirror m1
   !
  !
  default-action drop
 !
!
```

ICMP Message Example

This example displays the configuration for localized data policy for ICMP messages.

```
policy
access-list acl_1
 sequence 100
```

```
match
 protocol 1
 icmp-msg administratively-prohibited
!
action accept
 count administratively-prohibited
!
!
```