Policy Basics

- Policy Overview, on page 1
- Policies in Cisco vManage, on page 3

Policy Overview

Policy influences the flow of data traffic and routing information among Cisco vEdge devices and Cisco XE SD-WAN devices in the overlay network. Policy comprises:

- Routing policy—which affects the flow of routing information in the network's control plane
- Data policy—which affects the flow of data traffic in the network's data plane

To implement enterprise-specific traffic control requirements, you create basic policies, and you deploy advanced features of the Cisco SD-WAN software that are activated by means of the policy configuration infrastructure.

Just as the Cisco SD-WAN overlay network architecture clearly separates the control plane from the data plane and clearly separates control between centralized and localized functions, the Cisco SD-WAN policy software is cleanly separated. Policies apply either to control plane or data plane traffic, and they are configured either centrally (on Cisco vSmart Controllers) or locally (on Cisco vEdge devices and Cisco XE SD-WAN devices). The following figure illustrates the division between control and data policy, and between centralized and local policy.
Control and Data Policy

Control policy is the equivalent of routing protocol policy, and data policy is equivalent to what are commonly called access control lists (ACLs) and firewall filters.

Centralized and Localized Policy

The Cisco SD-WAN policy software design provides a clear separation between centralized and localized policy. In short, centralized policy is provisioned on the centralized Cisco vSmart Controllers in the overlay network, and the localized policy is provisioned on Cisco vEdge devices and Cisco XE SD-WAN devices, which sit at the network edge between a branch or enterprise site and a transport network, such as the Internet, MPLS, or metro Ethernet.

Centralized Policy

Centralized policy refers to policy provisioned on Cisco vSmart Controllers, which are the centralized controllers in the Cisco SD-WAN overlay network. Centralized policy comprises two components:

- Control policy, which affects the overlay network–wide routing of traffic
- Data policy, which affects the data traffic flow throughout the VPN segments in the network

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

Note

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

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

Note

These policies are pushed to the selected Cisco vEdge devices and the Cisco XE SD-WAN devices.

Localized Policy

Localized policy refers to a policy that is provisioned locally through the CLI on the Cisco vEdge devices and the Cisco XE SD-WAN devices, or through a Cisco vManage device template.

Localized control policy is also called as route policy, which affects (BGP and OSPF) routing behavior on the site-local network.

Localized data policy allows you to provision access lists and apply them to a specific interface or interfaces on the device. Simple access lists permit and restrict access based on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol), in the same way as with centralized data policy. Access lists also allow provisioning of class of service (CoS), policing, and mirroring, which control how data traffic flows out of and in to the device's interfaces and interface queues.
The design of the Cisco SD-WAN policy software distinguishes between basic and advanced policy. Basic policy allows you to influence or determine basic traffic flow through the overlay network. Here, you perform standard policy tasks, such as managing the paths along which traffic is routed through the network, and permitting or blocking traffic based on the address, port, and DSCP fields in the packet's IP header. You can also control the flow of data traffic into and out of a Cisco vEdge device's or a Cisco XE SD-WAN device's interfaces, enabling features such as class of service, queuing, and policing. Mirroring is available for Cisco vEdge devices.

Advanced features of Cisco SD-WAN policy software offer specialized policy-based network applications. Examples of these applications include the following:

- Service chaining, which redirects data traffic to shared devices in the network, such as firewall, intrusion detection and prevention (IDS), load balancer, and other devices, before the traffic is delivered to its destination. Service chaining obviates the need to have a separate device at each branch site.

- Application-aware routing, which selects the best path for traffic based on real-time network and path performance characteristics.

- Cflowd, for monitoring traffic flow.

- Converting a Cisco vEdge device into a NAT device, to allow traffic destined for the Internet or other public network can exit directly from the Cisco vEdge device.

By default, no policy of any kind is configured on Cisco XE SD-WAN devices, either on the centralized Cisco vSmart Controllers or the local Cisco vEdge devices and the Cisco XE SD-WAN devices. When control plane traffic, which distributes route information, is unpolicied:

- All route information that OMP propagates among the Cisco XE SD-WAN devices is shared, unmodified, among all Cisco vSmart Controllers and all Cisco vEdge devices and Cisco XE SD-WAN devices in the overlay network domain.

- No BGP or OSPF route policies are in place to affect the route information that Cisco vEdge devices and Cisco XE SD-WAN devices propagate within their local site network.

When data plane traffic is unpolicied, all data traffic is directed towards its destination based solely on the entries in the local Cisco vEdge device and the Cisco XE SD-WAN device's route table, and all VPNs in the overlay network can exchange data traffic.

This section examines the structural components of routing and data policy in the Cisco SD-WAN overlay network.

**Policies in Cisco vManage**

Use the Policies screen to create and activate centralized and localized control and data policies for Cisco vSmart Controllers, Cisco vEdge devices, and Cisco XE SD-WAN devices.

**Screen Elements**

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

- Title bar—Includes the title of the screen, Policies, and the following:
• Custom Options—Click to display, create, and edit a components for use in policy. For centralized policy, the components are CLI policies, lists, topologies, and traffic policies. For localized policy, the components are CLI policies, lists, forwarding class/QoS definitions, access control lists (ACLs), and route policies.

• Centralized Policy tab—Create a centralized policy. When you first open the Policies screen, the Centralized Policy tab is selected.
  • Add Policy—Click to create a centralized policy using a policy configuration wizard.

• Localized Policy tab—Create a localized policy.
  • Add Policy—Click to create a localized policy using a policy configuration wizard.

• Search box—Includes the Search Options drop-down, for a Contains or Match string.
• Refresh icon—Click to refresh data in the policies table with the most current data.
• Show Table Columns icon—Click to display or hide columns from the policies table. By default, all columns are displayed.
• Policies table—To re-arrange the columns, drag the column title to the desired position.

Configure Policies

• Configure Centralized Policy
• Configure Localized Policy
View a Policy
1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click View. Policies created with the UI policy builder are displayed in graphical format. Policies created using the CLI are displayed in text format.
3. Click Cancel to return to the policies table.

For a policy created using the vManage policy configuration wizard, you can view the policy in text format:
1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Preview.
3. Click Cancel to return to the policies table.

Copy a Policy
1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Copy.
3. In the Policy Copy popup window, enter the policy name and a description of the policy.

Note
If you are upgrading to 18.4.4, Data Policy names need to be under 26 characters.

Note
Starting Cisco SD-WAN release 19.3, the 127 characters are supported for policy names for the following policy types:
- Central route policy
- Local route policy
- Local Access Control (ACL)
- Local IPv6 ACL
- Central Data Policy
- Central App route policy
- QoS Map
- Rewrite Rule

All other policy names support 32 characters.
4. Click Copy.

Edit a Policy
For policies created using the vManage policy configuration wizard:
1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Save Policy Changes.

For policies created using the CLI:
1. In the Custom Options drop-down, click CLI Policy.
2. Click the More Actions icon to the right of the column and click Edit.
3. Edit the policy as needed.
4. Click Update.

Edit or Create a Policy Component
You can create individual policy components directly and then use them or import them when you are using the policy configuration wizard:
1. In the Title bar, click the Custom Options drop-down.
2. For centralized policy, select the policy component:
   • CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.
   • Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.
   • Topology—Create a hub-and-spoke, mesh, or custom topology or a VPN membership to import in the Topology screen in the policy configuration wizard.
   • Traffic Policy—Create an application-aware routing, traffic data, or cflowd policy to import in the Traffic Rules screen in the policy configuration wizard.

1. For localized policy, select the policy component:
   • CLI policy—Create the policy using the command-line interface rather than the policy configuration wizard.
   • Lists—Create groups of interest to import in the Group of Interest screen in the policy configuration wizard.
   • Forwarding Class/QoS—Create QoS mappings and rewrite rules to import in the Forwarding Classes/QoS screen in the policy configuration wizard.
   • Access Control Lists—Create ACLs of interest to import in the Configure Access Lists screen in the policy configuration wizard.
   • Route Policy—Create route policies to import in the Configure Route Policies screen in the policy configuration wizard.
Delete a Policy
1. In the Centralized Policy or Localized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Delete.
3. Click OK to confirm deletion of the policy.

Activate a Centralized Policy on Cisco vSmart Controllers
1. In the Centralized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Activate.
3. In the Activate Policy popup, click Activate to push the policy to all reachable Cisco vSmart Controllers in the network.
4. Click OK to confirm activation of the policy on all Cisco vSmart Controllers.

Deactivate a Centralized Policy on Cisco vSmart Controllers
1. In the Centralized Policy tab, select a policy.
2. Click the More Actions icon to the right of the column and click Deactivate.
3. In the Deactivate Policy popup, click Deactivate to confirm that you want to remove the policy from all reachable Cisco vSmart Controllers.
Policies in Cisco vManage