

Centralized Policy

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

- Overview of Centralized Policies, on page 1
- Configure Centralized Policies Using Cisco SD-WAN Manager, on page 2
- Configure Centralized Policies Using the CLI, on page 38
- Centralized Policies Configuration Examples, on page 42

Overview of Centralized Policies

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

Types of Centralized Policies

Centralized Control Policy

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

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

Centralized Data Policy

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

Centralized Data Policy Based on Packet Header Fields

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

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

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

Configure Centralized Policies Using Cisco SD-WAN Manager

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

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

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

To configure centralized policies using Cisco SD-WAN Manager, use the steps identified in the procedures that follow this section.

Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. Click **Add Policy**.

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

Configure Groups of Interest for Centralized Policy

In **Create Groups of Interest**, create new groups of list types as described in the following sections to use in a centralized policy:

Configure Application

1. In the groups of interest list, click **Application** list type.
2. Click **New Application List**.
3. Enter a name for the list.
4. Choose either **Application** or **Application Family**.

   Application can be the names of one or more applications, such as **Third Party Control**, **ABC News**, **Mircosoft Teams**, and so on. The Cisco IOS XE Catalyst SD-WAN devices support about 2300 different applications. To list the supported applications, use the **?** in the CLI.

   Application Family 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**.
5. In the **Select** drop-down, in the 'Search' filter, select the required applications or application families.
6. Click **Add**.

A few application lists are preconfigured. You cannot edit or delete these lists.

Microsoft_Apps—Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the Entries column.

Google_Apps—Includes Google applications, such as Gmail, Google maps, and YouTube. To display a full list of Google applications, click the list in the Entries column.

Configure Color

1. In the groups of interest list, click **Color**.
2. Click **New Color List**.
3. Enter a name for the list.
4. In the **Select Color** drop-down, in the 'Search' filter select the required colors.

   Colors 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.
5. Click **Add**.

To configure multiple colors in a single list, you can select multiple colors from the drop-down.

Configure Community

Table 1: Feature History

Feature Name	Release Information	Description
Ability to Match and Set Communities	Cisco SD-WAN Release 20.5.1 Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature lets you match and set communities using a control policy. Control policies are defined and applied on Cisco IOS XE Catalyst SD-WAN device devices to manipulate communities. With this feature, you can match and assign single or multiple BGP community tags to your prefixes based on which routing policies can be manipulated.

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

1. In the group of interest list, click **Community**.
2. Click **New Community List**.
3. Enter a name for the community list.
4. Choose either **Standard** or **Expanded**.
   - Standard community lists are used to specify communities and community numbers.
   - Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to specify patterns to match community attributes.
5. In the **Add Community** field, enter one or more data prefixes separated by commas in any of the following formats:
   - *aa*:*nn*: Autonomous System (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 number.
   - **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.
   - **no-export**: Attaches 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.
6. Click **Add**.

Configure Data Prefix

1. In the **Groups of Interest** list, click **Data Prefix**.

2. Click **New Data Prefix List**.
3. Enter a name for the list.
4. Choose either **IPv4** or **IPv6**.
5. In the **Add Data Prefix** field, enter one or more data prefixes separated by commas.
6. Click **Add**.

Configure Policer

1. In the groups of interest list, click **Policer**.
2. Click **New Policer List**.
3. Enter a name for the list.
4. Define the policing parameters:
   a. In the **Burst** field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes.
   b. 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**.
   c. In the **Rate** field, enter the maximum traffic rate, a value from 0 through $2^{64} - 1$ bits per second (bps).
5. Click **Add**.

Note For ACL or data policy, even if the same policer object is used in different sequences, each sequence is policed separately. For example, consider that policer rate is 1000000 or 1Mb. If the same policer is set for multiple sequences then each sequence polices 1Mb traffic. If there are different policers configured for difference sequences, then each policer polices traffic based on the respective policing rate.

Configure Prefix

1. In the groups of interest list, click **Prefix**.
2. Click **New Prefix List**.
3. Enter a name for the list.
4. In the **Add Prefix** field, enter one or more data prefixes separated by commas.
5. Click **Add**.

Configure Site

1. In the groups of interest list, click **Site**.
2. Click **New Site List**.

3. Enter a name for the list.
4. In the **Add Site** field, enter one or more site IDs separated by commas.

   For example, 100 or 200 separated by commas or in the range, 0 - 4294967295.
5. Click **Add**.

Configure App Probe Class

1. In the groups of interest list, click **App Probe Class**.
2. Click **New App Probe Class**.
3. Enter the probe class name in the **Probe Class Name** field.
4. Select the required forwarding class from the **Forwarding Class** drop-down list.
5. In the **Entries** pane, select the appropriate color from the **Color** drop-down list and enter the **DSCP** value.

   You can add more entries if needed by clicking on the **+** symbol.
6. Click **Save**.

Configure SLA Class

1. In the groups of interest list, click **SLA Class**.
2. Click **New SLA Class List**.
3. Enter a name for the list.
4. Define the SLA class parameters:
   a. In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.
   b. In the **Latency** field, enter the maximum packet latency on the connection, a value from 0 through 1,000 milliseconds.
   c. In the **Jitter** field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
   d. Select the required app probe class from the **App Probe Class** drop-down list.
5. (Optional) Select the **Fallback Best Tunnel** checkbox to enable the best tunnel criteria.

   This optional filed is available from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a to pick the best path or color from the available colors when SLA is not met. When this option is selected, you can choose the required criteria from the drop-down. The criteria are a combination of one or more of losses, latency, and, jitter values.
6. Select the **Criteria** from the drop-down list. The available criteria are:
   - Latency
   - Loss
   - Jitter

- Latency, Loss
- Latency, Jitter
- Loss, Latency
- Loss, Jitter
- Jitter, Latency
- Jitter, Loss
- Latency, Loss, Jitter
- Latency, Jitter, Loss
- Loss, Latency, Jitter
- Loss, Jitter, Latency
- Jitter, Latency, Loss
- Jitter, Loss, Latency

7. Enter the **Loss Variance (%)**, **Latency Variance (ms)**, and the **Jitter Variance (ms)** for the selected criteria.
8. Click **Add**.

Configure TLOC

1. In the groups of interest list, click **TLOC**.
2. Click **New TLOC List**. The **TLOC List** popup displays.
3. Enter a name for the list.
4. In the **TLOC IP** field, enter the system IP address for the TLOC.
5. In the **Color** field, select the TLOC's color.
6. In the **Encap** field, select the encapsulation type.
7. In the **Preference** field, optionally select a preference to associate with the TLOC.

   The range is 0 to 4294967295.
8. Click **Add TLOC** to add another TLOC to the list.
9. Click **Save**.



Note To use the `set tloc` and `set tloc-list` commands, you must use the set-vpn command.

For each TLOC, specify its address, color, and encapsulation. 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 TLOCs have the highest preference value, traffic is sent among them in an ECMP fashion.

If IPsec preference is set on the local preferred color for an edge router, the local TLOC and the color does not overlap with the centralized policy configured with local color preference. The edge router with local TLOC preference takes the precedence. In this case, the preferred TLOC configured in centralized policy is not considered.

Configure VPN

1. In the groups of interest list, click **VPN**.
2. Click **New VPN List**.
3. Enter a name for the list.
4. In the **Add VPN** field, enter one or more VPN IDs separated by commas.

   For example, 100 and 200 separated by commas. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
5. Click **Add**.

Configure Region

Minimum release: Cisco vManage Release 20.7.1

To configure a list of regions for Multi-Region Fabric (formerly Hierarchical SD-WAN), ensure that Multi-Region Fabric is enabled in **Administration** > **Settings**.

1. In the groups of interest list, click **Region**.
2. Click **New Region List**.
3. In the **Region List Name** field, enter a name for the region list.
4. In the **Add Region** field, enter one or more regions, separated by commas, or enter a range.

   For example, specify regions 1, 3 with commas, or a range 1-4.
5. Click **Add**.

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

Configure Preferred Color Group

Table 2: Feature History

Feature Name	Release Information	Description
Tiered Transport Preference in Application-aware Routing and Data Policy	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature adds support for ranking of Application Aware Routing (AAR) preferred and backup preferred colors. You can configure up to three levels of priority based on the color or path preference on a Cisco IOS XE Catalyst SD-WAN device.

You can configure the order of transport preference to choose the preference order for forwarding traffic.

The **Preferred Color Group** is supported only on overlay traffic but not on DIA traffic.

1. In the groups of interest list, click **Preferred Color Group**.
2. Click **New Preferred Color Group**.
3. In the **Preferred Color Group Name** field, enter a name for the preferred color group.
4. In the **Primary Colors** pane, do the following:
   a. Choose the color preference from the **Color Preference** drop-down list.
   b. Choose the path preference from the **Path Preference** drop-down list.

Field	Description
Preferred Color Group Name	Enter a name of the preferred color group.
Color Preference	Choose the color preference from the drop-down list. The options are: • default • 3g • biz-internet • blue • bronze • custom1 • custom2, and so on You can select multiple colors.
Path Preference	Choose the path preference from the drop-down list. The options are: • Direct Path: Use only a direct path between the source and the destination devices. • Multi Hop Path: In a Multi-Region Fabric network, use a multi-hop path, which includes the core region, between the source and destination devices, even if a direct path is available. • All Paths: Use any path between the source and destination devices. **Note** This option is equivalent to not configuring path preference at all. If you are applying the policy to a non-Multi-Region Fabric network, use this option.

5. In the **Secondary Colors** pane, do the following:
   a. Choose the color preference in the **Color Preference** drop-down list.
   b. Choose the path preference from the **Path Preference** drop-down list.

6. In the **Tertiary Colors** pane, do the following:
   a. Choose the color preference from the **Color Preference** drop-down list.
   b. Choose the path preference from the **Path Preference** drop-down list.
7. Click **Add**.

The following guidelines are helpful when configuring the ranking for colors:

- Primary preference is mandatory, and at each priority level, at least one preference path or color is mandatory. Both can also be configured.
- More than one color can be configured as a preference.
- If path preference is not configured, all paths are constrained by the preferred colors that are available.
- If color preference is not configured within the constraint of the path preference, then all the colors are available.
- The preferences apply in order of priority to determine the path or color for forwarding traffic.

When the primary, secondary, and tertiary colors are down, packets are not dropped. The traffic falls back to the usual routing preference to choose if any other colors are up.

Integrating WAN Insight (WANI) into Cisco SD-WAN Manager

Table 3: Feature History

Feature Name	Release Information	Description
WAN Insight Policy Automation	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	With this feature, you can apply the recommendations that are available on Cisco SD-WAN Analytics toCisco SD-WAN Manager AAR policy and view the applied recommendations on Cisco SD-WAN Manager.

Cisco SD-WAN Analytics is a cloud-based analytics service for Cisco Catalyst SD-WAN offering comprehensive insights into application and network performance. The analytics service is available with Cisco DNA Advantage and Cisco DNA Premier software subscriptions. Cisco SD-WAN Analytics collects and stores metadata about traffic flows in its cloud storage and produces analytics based on this collected data. Predictive Path Analytics generates recommendations for path based on long term insights. These recommendations need to be converted into policy created manually on Cisco SD-WAN Manager and then applied to the network.

The Predictive Path Recommendations feature allows you to apply active recommendations to the actionable centralized AAR policy to influence the forwarding decisions in the Cisco Catalyst SD-WAN network. The recommendations are applied as a part of the AAR policy and then pushed to Cisco SD-WAN Controller. The Predictive Path Recommendations are applied to the SD-WAN network as TLOC preferences in AAR policies.

For more information about using Predictive Path Recommendations, see Predictive Path Recommendations.

Apply Predictive Path Recommendations

When there are predictive path recommendations in Cisco SD-WAN Analytics, perform the following steps to apply the recommendations to the Application-Aware routing policies:

1. In the Cisco SD-WAN Manager menu, click the bell icon at the top-right corner. The **Notifications** pane is displayed with active alarms.
2. If there are any **Active Recommendations** in the **Notifications** pane, click on the site to view the recommendations. Alternatively, you can view from the Cisco SD-WAN Manager menu, click **Analytics** > **Predictive Networks**.
3. Click **Active Recommendations**, and then click **Apply**.
4. In the **Apply Predictive Path Recommendations** window, click **Proceed to Apply** to apply new recommendations.

   You can review the applied recommendations in the Cisco SD-WAN Manager generated configs and push the recommendations to Cisco SD-WAN Controller.

Points to Consider

- Cisco SD-WAN Manager pulls recommendations when you log in. If you want to update the recommendations, refresh the page or log in again.
- Cisco SD-WAN Manager support recommendations for application lists which are associated with some AAR policy only. If AAR Policy does not exist for a given application list, the recommendations are not valid and policy processing is not done.
- WAN Insights generates recommendations for standard App Groups even when the AAR Policy is not defined. However, the policy automation is not done since AAR policy is not defined.
- When for the same site and application list, if WANI generates a terminate for a recommendation which is applied and also generates another recommendation, the recommendations are applied based on the preferences.
- Application of WANI recommendations for Cloud OnRamp for SaaS is not supported.

Predictive Path Recommendations

WAN Insights (WANI) allows you to track the performance of your current network setup and tune your policies and paths to achieve the best user experience. Predictive path recommendations influence AAR policy TLOC preferences.

WAN Insights is a predictive network optimization tool that uses a statistical model to examine historical data from Cisco Catalyst SD-WAN, in order to find the best paths for application traffic. WANI analyzes the telemetry data exported during application traffic flows, and then generates long-term recommendations for paths that would reduce the probability of experiencing an SLA violation (for example, low-quality performance).

Predictive network associates some SLA with each application list that is defined in the AAR policy in order to detect SLA violations for the applications. This is used to calculate a probability of SLA violation on a given site and TLOC and generates recommendations.

For more information about configuring group of interest for data policies, see Configure Groups of Interest for Centralized Policy.

Configure Topology and VPN Membership

When you first open the **Configure Topology and VPN Membership** window, the **Topology** window is displayed by default.

To configure topology and VPN membership:

Hub-and-Spoke

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

Mesh

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

8. Click **Add**.
9. Repeat these steps to add more mesh regions to the policy.
10. Click **Save Mesh Topology**.

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

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

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

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

12. Click **Sequence Type** to configure more sequences, as desired. Drag and drop to re-order them.
13. Click **Save Control Policy**.

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

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.

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

Note The Cisco Catalyst SD-WAN policy supports maximum up to 1024 sequences, including default sequence.

Default Action

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

If a selected data packet 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.

Import Existing Topology

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

Note The policy configuration wizard does not let you import an already configured policy as in other instances of centralized policies (data, control, or application-aware routing). The policy must be configured in its entirety.

5. Click **Import**.

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

Create a VPN Membership Policy

1. In the **Specify your network topology** area, click **VPN Membership**.
2. Click **Add VPN Membership Policy**.

Note You can add only one VPN membership at a time, therefore all site lists and VPN lists must be included in a single policy.

The **Add VPN Membership Policy** popup displays.

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

Configure Traffic Rules

Table 4: Feature History

Feature Name	Release Information	Description
Policy Matching with ICMP Message	Cisco IOS XE Release 17.4.1 Cisco vManage Release 20.4.1	This feature provides support for a new match condition that you can use to specify a list of ICMP messages for centralized data policies, localized data policies, and Application-Aware Routing policies.

When you first open the **Configure Traffic Rules** window, **Application-Aware Routing** is selected by default.

You can also view already created AAR routing policies listed in the page. It provides various information related to the policies such as the Name of the policy, Type, Mode, Description, Update By, and Last Updated details.

Note You can refer to the Mode column for the security status details of the policy. The status helps to differentiate whether the policy is used in unified security or not. The mode status is applicable only for security policies and not relevant to any centralized or localized policies.

For more information on configuring traffic rules for the Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) flow, see Cisco Catalyst SD-WAN Application Intelligence Engine Flow.

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

To configure traffic rules for a centralized data policy:

1. Click **Traffic Data**.
2. Click the **Add Policy** drop-down.
3. Click **Create New**. The **Add Data Policy** window displays.
4. Enter a name and a description for the data policy.
5. In the right pane, click **Sequence Type**. The **Add Data Policy** popup opens.
6. Select the type of data policy you want to create, **Application Firewall**, **QoS**, **Traffic Engineering**, or **Custom**.



Note If you want to configure multiple types of data policies for the same match condition, you need to configure a custom policy.

7. A policy sequence containing the text string **Application**, **Firewall**, **QoS**, **Traffic Engineering**, or **Custom** is added in the left pane.
8. Double-click the text string, and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.
9. In the right pane, click **Sequence Rule**. The **Match/Action** box opens, and **Match** is selected by default. The available policy match conditions are listed below the box.



Note Adding multiple application matches, subnet matches, or combining several match conditions in a single sequence may increase the total filter count beyond the allowed maximum.

If this total filter count is reached, an error message `Filter count exceeded MAX (64)` is displayed when applying a data policy configuration.

Match Condition	Procedure
None (match all packets)	Do not specify any match conditions.

Match Condition	Procedure
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**. This match condition is available for IPv6 traffic from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1.
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.
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 [-]).
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. This match condition is available for IPv6 traffic from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco vManage Release 20.9.1.
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.
DSCP	**a.** In the **Match** conditions, click **DSCP**. **b.** In the **DSCP** field, type the DSCP value, a number from 0 through 63.

Match Condition	Procedure
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.
PLP	**a.** In the **Match** conditions, click **PLP** to set the **Packet Loss Priority**. **b.** In the **PLP** drop-down, select **Low** or **High**. To set the PLP to **High**, apply a policer that includes the **exceed remark** option.
Protocol	**a.** In the **Match** conditions, click **Protocol**. **b.** In the **Protocol** field, type the Internet Protocol number, a number from 0 through 255.
ICMP Message	To match ICMP messages, in the Protocol field, set the Internet Protocol Number to 1, or 58, or both. **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1.
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 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 [-]).
TCP	**a.** In the **Match** conditions, click **TCP**. **b.** In the **TCP** field, **syn** is the only option available.

10. For QoS and Traffic Engineering data policies: From the **Protocol** drop-down list, select **IPv4** to apply the policy only to IPv4 address families, **IPv6** to apply the policy only to IPv6 address families, or **Both** to apply the policy to IPv4 and IPv6 address families.
11. To select one or more **Match** conditions, click its box and set the values as described.

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

12. To select actions to take on matching data traffic, click the **Actions** box.
13. To drop matching traffic, click **Drop**. The available policy actions are listed in the right side.
14. To accept matching traffic, click **Accept**. The available policy actions are listed in the right side.
15. Set the policy action as described.

Note Not all actions are available for all match conditions.

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
   !
  !
```

Action 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	Minimum release: Cisco vManage Release 20.11.1 and Cisco IOS XE Release 17.11.1a 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.	**a.** In the **Action** conditions, click **Log** to enable logging.

Action Condition	Description	Procedure
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.
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. If you choose **FEC Adaptive**, an additional field, **Loss Threshold**, displays that allows you to specify the packet loss threshold for automatically enabling FEC. Adaptive FEC starts to work at 2% packet loss; this value is configurable. You can specify a loss threshold of 1 to 5%. The default packet loss threshold is 2%. • **FEC Always** – Corresponding packets are always subjected to FEC. • **Packet Duplication** – Sends duplicate packets over a single tunnel. If more than one tunnel is available, duplicated packets will be sent over the tunnel with the best parameters.	**a.** In the **Match** conditions, click **Loss Correction**. **b.** In the **Loss Correction** field, select **FEC Adaptive**, **FEC Always**, or **Packet Duplication**.
Click **Save Match and Actions**.		

16. Create additional sequence rules as desired. Drag and drop to re-arrange them.
17. Click **Save Data Policy**.
18. Click **Next** to move to **Apply Policies to Sites and VPNs** in the wizard.

Match Parameters - Control Policy

For OMP and TLOC routes , you can match the following attributes:

Match Condition	Description
Color List	One or more colors. 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.
Community List	List of one or more BGP communities. In the **Community List** field, 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.
Types	Specifies the community type. Choose **Standard** to specify communities and community numbers or, **Expanded** to filter communities using a regular expression. Regular expressions are used to specify patterns to match community attributes.
Criteria OR	Compares each regex string in the community list against the community string of the route. The OR condition is applicable across multiple community lists and is valid for all devices. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the Community **Types** and **Criteria** fields are available.
OMP Tag	Tag value associated with the route or prefix in the routing database on the device. The range is 0 through 4294967295.
Origin	Protocol from which the route was learned.
Originator	IP address from which the route was learned.

Match Condition	Description
Path Type	In a Hierarchical SD-WAN architecture, match a route by its path type, which can be one of the following: • **Hierarchical Path**: A route that includes hops from an access region to a border router, through region 0, to another border router, then to an edge router in a different access region • **Direct Path**: A direct path route from one edge router to another edge router. • **Transport Gateway Path**: A route that is re-originated by a router that has transport gateway functionality enabled. **Note** This option is available beginning with Cisco vManage Release 20.8.1.
Preference	How preferred a prefix is. This is the preference value that the route or prefix has in the local site, that is, in the routing database on the device. A higher preference value is more preferred.The range is 0 through 255.
Prefix List	One or more prefixes. Specifies the name of a prefix list.
Not available in Cisco SD-WAN Manager.	One or more overlay network site identifiers.
Site	Individual site identifier. The range is 0 through 4294967295.
Region	Region defined for Hierarchical SD-WAN. The range is 1 to 63. **Note** This option is available beginning with Cisco vManage Release 20.7.1.
Role	In a Hierarchical SD-WAN architecture, match by the device type, which can be **Border Router** or **Edge Router**. **Note** This option is available beginning with Cisco vManage Release 20.8.1.

Match Condition	Description
TLOC	Individual TLOC address. **Note** To use the `set tloc` and `set tloc-list` commands, you must use the set-vpn command.
VPN	Individual VPN identifier. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here. When a policy is pushed with duplicate VPN IDs, the latest VPN ID overwrites the first one. However, starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.5, the first one is not overridden.
Carrier	Carrier for the control traffic. Values are: default, carrier1 through carrier8.
Domain ID	Domain identifier associated with a TLOC. The range is 0 through 4294967295.
OMP Tag	Tag value associated with the TLOC route in the route table on the device. The range is 0 through 4294967295.
Site	Individual site contributor or more overlay network site identifiers.. The range is 0 through 4294967295.

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

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 5:

Match Condition	Description
Omit	Match all packets.
Applications/Application Family List	Applications or application families. This match condition is available for IPv6 traffic from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1.

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. This match condition is available for IPv6 traffic from Cisco IOS XE Release 17.9.1a and Cisco vManage Release 20.9.1.
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 IOS XE Release 17.4.1, Cisco vManage Release 20.4.1.
Source Data Prefix	Specifies the group of source prefixes or an individual source prefix.

Match Condition	Description
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.
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 6: 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 7: 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 - Control Policy

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

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

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

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

Table 8:

Description	Cisco SD-WAN Manager
Accept the route. An accepted route is eligible to be modified by the additional parameters configured in the **action** portion of the policy configuration.	Click **Accept**.
Discard the packet.	Click **Reject**.

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

Action Condition	Description
Export To	Export the route the the specified VPN or list of VPNs (for a **match route** match condition only). The range is 0 through 65535 or list name.
OMP Tag	Change the tag string in the route, prefix, or TLOC. The range is 0 through 4294967295.
Preference	Change the preference value in the route, prefix, or TLOC to the specified value. A higher preference value is more preferred. The range is 0 through 255.
Service	Specify a service to redirect traffic to before delivering the traffic to its destination. The TLOC address or list of TLOCs identifies the TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Standard services: **FW**, **IDS**, **IDP** Custom services: **netsvc1**, **netsvc2**, **netsvc3**, **netsvc4** Configure the services themselves on the Cisco IOS XE Catalyst SD-WAN devices that are collocated with the service devices, using the **vpn service** configuration command.
TLOC	Change the TLOC address, color, and encapsulation to the specified address and color. 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**, **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.

Action Condition	Description
TLOC Action	Direct matching routes or TLOCs using the mechanism specified by *action*, and enable end-to-end tracking of whether the ultimate destination is reachable. Setting the TLOC action option enables the Cisco Catalyst SD-WAN Controller to perform end-to-end tracking of the path to the ultimate destination device.



Note The **preference** command controls the preference for directing inbound and outbound traffic to a tunnel. The preference can be a value from 0 through 4294967295 (232 – 1), and the default value is 0. A higher value is preferred over a lower value.

When a Cisco vEdge device has two or more tunnels, if all the TLOCs have the same preference and no policy is applied that affects traffic flow, all the TLOCs are advertised into OMP. When the router transmits or receives traffic, it distributes traffic flows evenly among the tunnels, using ECMP.

Action Parameters - Data Policy

Table 9: 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 IOS XE Release 17.4.1 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 IOS XE Catalyst SD-WAN Release 17.5.1a 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 IOS XE Catalyst SD-WAN 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.
Traffic Redirection to SIG Using Data Policy: Fallback to Routing	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	With this feature, you can configure internet-bound traffic to be routed through the Cisco Catalyst SD-WAN overlay, as a fallback mechanism, when all SIG tunnels are down.

Feature Name	Release Information	Description
Log Action for both Localized and Centralized Data Policies	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature enables you to set a log action parameter for data policy, application route policy, and localized policy while configuring data policies on Cisco IOS XE Catalyst SD-WAN devices. The log parameter allows packets to get logged and generate syslog messages. Logs are exported to an external syslog server every five minutes when a flow is active. You can control policy logs as per the configured rate using the command **policy log-rate-limit**.
Remote Preferred Color in Data Policy	Cisco IOS XE Catalyst SD-WAN Release 17.15.1aCisco Catalyst SD-WAN Manager Release 20.15.1	You can set a remote preferred color in the data policy to control traffic routing based on the SLA criteria. See Configure traffic rules using classic policies for more information.

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 IOS XE Catalyst SD-WAN device.
Click **Drop**	Discards the packet. This is the default action.
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.

Action Condition	Description
Redirect DNS	Redirects DNS requests to a particular DNS server or Umbrella. 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. **redirect-dns umbrella** is only supported in Direct Internet Interface (DIA) use cases. It is not supported in SIG/SSE or overlay scenarios. When using **redirect-dns umbrella**, you do not need to explicitly configure **nat use-vpn 0**. **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.
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. Check the **Fallback to Routing** check box to route internet-bound traffic through the Cisco SD-WAN overlay when all SIG tunnels are down. This option is introduced in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1.

Note On Cisco IOS XE Catalyst SD-WAN devices, all the ongoing optimized flows are dropped when the TCP Optimization is removed.

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. You can configure up to 31 (1–31) NAT pools per router.
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 IOS XE Catalyst SD-WAN Release 17.5.1a 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 IOS XE Catalyst SD-WAN 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. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.



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 10:

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)

IPv4 Actions	IPv6 Actions
App-Route backup-preferred color, local-tloc, local-tloc-list	App-Route backup-preferred color, local-tloc, local-tloc-list

Apply Policies to Sites and VPNs

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

1. In the **Policy Name** field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
2. In the **Policy Description** field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.
3. Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:
   a. For a **Topology** policy block, click **New Site List**, **Inbound Site List**, **Outbound Site List**, or **VPN List**. Some topology blocks might have no **Add** buttons. Choose one or more site lists, and choose one or more VPN lists. Click **Add**.
   b. For an **Application-Aware Routing** policy block, click **New Site List** and **VPN list**. Choose one or more site lists, and choose one or more VPN lists. Click **Add**.
   c. For a **Traffic Data** policy block, click **New Site List and VPN List**. Choose the direction for applying the policy (**From Service**, **From Tunnel**, or **All**), choose one or more site lists, and choose one or more VPN lists. Click **Add**.
   d. For a cflowd policy block, click **New Site List**. Choose one or more site lists, and click **Add**.
4. Click **Preview** to view the configured policy. The policy appears in CLI format.
5. Click **Save Policy**. The **Configuration** > **Policies** page appears, and the policies table includes the newly created policy.

NAT Fallback on Cisco IOS XE Catalyst SD-WAN Devices

	Release Information	
NAT Fallback on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Release 17.3.2 Cisco vManage Release 20.3.2	Cisco IOS XE Catalyst SD-WAN devices support the NAT fallback feature for Direct Internet Access (DIA). The NAT fallback feature provides a routing-based mechanism for all traffic that is sent to the DIA route to use an alternative route when required. With this release, fallback is supported on the service and tunnel side.

Note To use Cisco SD-WAN Manager to configure NAT DIA fallback, Cisco SD-WAN Manager must manage your Cisco Catalyst SD-WAN Controller.

To enable NAT fallback using Cisco SD-WAN Manager, create and configure a data policy by doing the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. From the **Custom** options drop-down, under **Centralized Policy**, select **Traffic Policy**.
3. Click **Traffic Data**.
4. From the **Add Policy** drop-down, click**Create New**.
5. Click **Sequence Type** and select **Custom**.
6. Click **(+) Sequence Rule** to create a new sequence rule.
7. After adding match conditions, click **Actions** and click **Accept**.
8. Click **NAT VPN** and select the **Fallback** checkbox.
9. Click **Save and Match Actions**.
10. Click **Save Data Policy**.

Edit your existing centralized policy and import the policy:

1. Click **Centralized Policy** and for the required centralized policy, click **...** and select **Edit**.
2. Click **Traffic Rules** and select **Traffic Data**.
3. From the **Add Policy** drop-down, select **Import Existing**.
4. Select the NAT policy that you created from the **Policy** drop-down.
5. Click **Policy Application** and select **Traffic Data**.
6. Click **+ New Site List and VPN List**.
7. Select the direction, VPN, and site as required.
8. Click **Add**.
9. Click **Save Policy Changes**.
10. Click to select **VPN**, and **Site** from the drop-down.

Note Policy configured for the **from-tunnel** traffic is also applied to the return DIA (Underlay) traffic apart from the return traffic coming over the tunnel. If none of the sequences in that policy match, it matches the default sequence in that policy.

Note The following NAT fallback actions/commands are now supported:

- Action: `nat fallback`
- When applying a policy: `direction from-tunnel`

Activate a Centralized Policy

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

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**. **Centralized Policy** is selected and displayed by default.
2. For the required policy, click **...** and select **Activate**. The **Activate Policy** popup appears. It lists the IP addresses of the reachable Cisco SD-WAN Controllers to which the policy must be applied.
3. Click **Activate**.

View Centralized Policies

To view centralized policies:

1. From the **Centralized Policy**, select a policy.
2. For a policy created using the UI policy builder or using the CLI, click **...** and select **View**. The policy created using the UI policy builder is displayed in graphical format while the policy created using the CLI method is displayed in text format.
3. For a policy created using Cisco SD-WAN Manager policy configuration wizard, click **...** and select **Preview**. This policy is displayed in text format.

Copy, Edit, and Delete Policies

To copy a policy:

1. From the **Centralized Policy**, select a policy.
2. For the desired policy, click **...** and select **Copy**.
3. In the Policy Copy popup window, enter the policy name and a description of the policy.

Note Starting with the Cisco IOS XE Release 17.2, 127 characters are supported for policy names for the following policy types:

- Central route policy
- Local route policy
- Local Access Control lOst (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**.

To edit policies created using the Cisco SD-WAN Manager policy configuration wizard:

1. For the desired policy, click **...** and select **Edit**.
2. Edit the policy as needed.
3. Click **Save Policy Changes**.

To edit polices created using the CLI method:

1. In the **Custom Options** drop-down, click **CLI Policy**.
2. For the desired policy, click **...** and select **Edit**.
3. Edit the policy as needed.
4. Click **Update**.

To delete policies:

1. From the **Centralized Policy**, select a policy.
2. For the desired policy, click **...** and select **Delete**.
3. Click **OK** to confirm deletion of the policy.

Configure Centralized Policies Using the CLI

To configure a centralized control policy using the CLI:

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

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

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

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

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

```
vsmart(config)# policy lists data-ipv6-prefix-list dest_ip_prefix_list
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# ipv6-prefix 2001:DB8::/32
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# commit
Commit complete.
```

```
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match destination-data-ipv6-prefix-list dest_ip_prefix_list
vsmart (config-match)# commit
vsmart(config-match)# exit
vsmart(config-sequence-100)# match source-data-ipv6-prefix-list dest_ip_prefix_list
vm9(config-match)# commit
Commit complete.
vm9(config-match)# end
```

```
vsmart(config)# policy
vsmart(config-policy)#  data-policy data_policy_1
vsmart(config-data-policy-data_policy_1)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 101
vsmart(config-sequence-101)# match source-ipv6 2001:DB8::/32
vsmart(config-match)# exit
vsmart(config-sequence-101)# match destination-ipv6 2001:DB8::/32
vsmart(config-match)#
```

3. Create a control policy instance:

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

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

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

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

5. Define match parameters for routes and for TLOCs:

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

6. Define actions to take when a match occurs:

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

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

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

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

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

Note Match origin command is available only for Cisco vEdge devices but not on Cisco IOS XE Catalyst SD-WAN devices.

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

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

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

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

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

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

```
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1 sequence 100
vsmart(config-sequence-100)# action accept set next-hop-ipv6 2001:DB8::/32
vsmart(config-set)#
```

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

service becomes unavailable, the Cisco IOS XE Catalyst SD-WAN device withdraws the service advertisement.

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

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

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

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

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

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

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

```
vsmart(config)# policy lists data-ipv6-prefix-list dest_ip_prefix_list
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# ipv6-prefix 2001:DB8:19::1
vsmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# commit
Commit complete.
```

```
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match destination-data-ipv6-prefix-list dest_ip_prefix_list
vsmart (config-match)# commit
vsmart(config-match)# exit
vsmart(config-sequence-100)# match source-data-ipv6-prefix-list dest_ip_prefix_list
vm9(config-match)# commit
Commit complete.
vm9(config-match)# end
```

```
vsmart(config)# policy
vsmart(config-policy)# data-policy data_policy_1
vsmart(config-data-policy-data_policy_1)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 101
vsmart(config-sequence-101)# match source-ipv6 2001:DB8:19::1
vsmart(config-match)# exit
vsmart(config-sequence-101)# match destination-ipv6 2001:DB8:19::1
vsmart(config-match)#
```

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
```

```
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1 sequence 100
vsmart(config-sequence-100)# action accept set next-hop-ipv6 2001:DB8:19::1
vsmart(config-set)#
```

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

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

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

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

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

Centralized Policies Configuration Examples

This topic provides some examples of configuring a centralized data policy to influence traffic flow across the Cisco IOS XE Catalyst SD-WAN domain and to configure a Cisco IOS XE 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 IOS XE 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
  !
 !
!
```

Then, apply this policy to the site list named **test-site-list**, which includes site 500:

```
vm9# show sdwan running-config apply-policy
apply-policy
 site-list test-site-list
  data-policy test-data-policy
 !
!
```

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

```
vm5# show sdwan 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
```

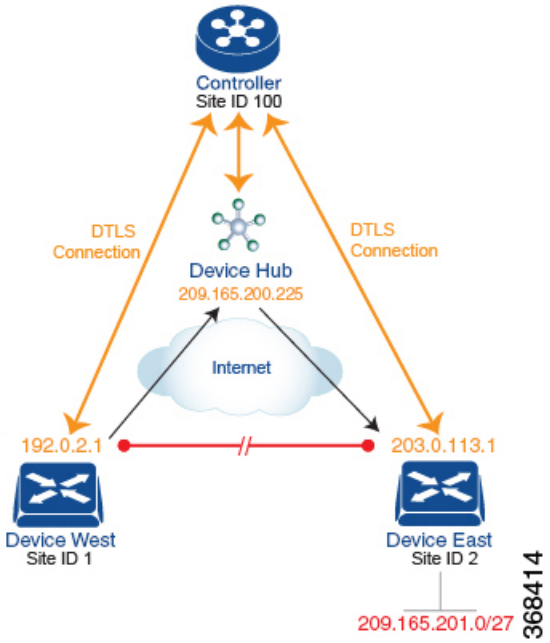
Traffic Engineering

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

One common way to design a domain in a Cisco IOS XE Catalyst 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 IOS XE Catalyst 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:

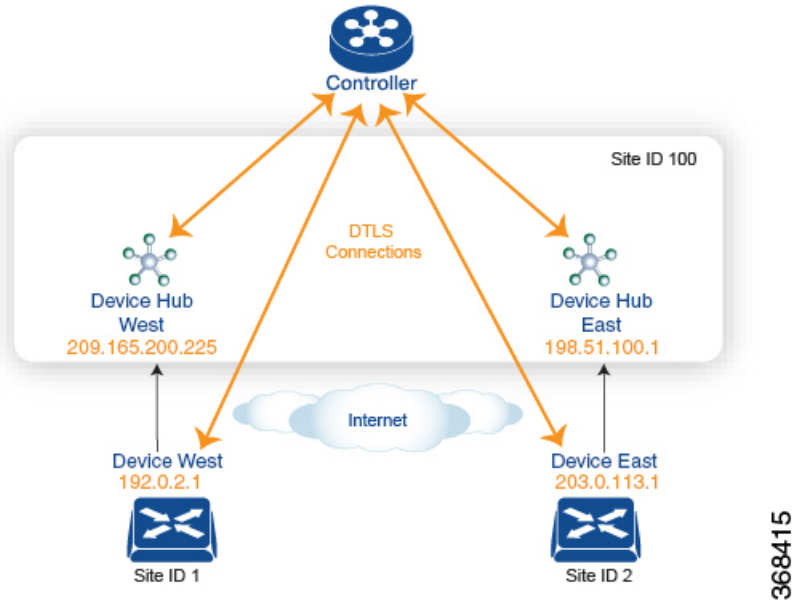
```
policy
  lists
    prefix-list east-prefixes
      ip-prefix 209.165.201.0/27
    site-list west-sites
      site-id 1
      site-id 11
      site-id 12
      site-id 13
```

```
  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.

Community Example

This example displays the configuration for centralized control policy for community lists.

```
policy
  lists
   expanded-community-list test
    community 0:110* 100:[7-9]+
```

```
    community 0:110* 11:*

   community-list test-com
    community 0:1
    community 0:2

control-policy test
  sequence 10
   match route
    expanded-community-list test

   action accept
    set
     community 100:2 100:3
     additive
```

This example displays the configuration for standard community lists.

```
Standard Community list

route : 0:1234 0:11 0:12

community-list
   community 0:100
   community 0:1234
   community 0:101
*MATCH*

route : 0:1234 0:11 0:12
community-list
  community 0:100
  community 0:5678
  community 0:101
*NO MATCH*
```

This example displays the configuration for expanded community lists. OR match compares each regex string in the community list against the route's community string.

```
Expanded Community list
route - 0:1234  0:5678
expanded-community-list:
  community 0:110* 11:
  community 0:110* 100:[7-9]+
  community 0:12[3-7]+
*MATCH*

route - 0:1234  0:5678
expanded-community-list:
   community 0:111*
   community 0:110* 11:*
*NO MATCH*
```

EXACT match input strings need to have communities in sorted order. Sorts it by byte value and add the meta characters for start and end of string.

```
route - 0:1234 0:5678
expanded-community-list:
community ^0:1234 0:5678$
*MATCH*
```

AND match input strings need to have communities in sorted order. Add '.+' to blindly match between the sorted communities.

```
route - 0:0 0:1234  0:5678  0:9789 0:9800 0:9900 0:9999 1:10
```

```
expanded-community-list:
   community 0:1234 .+ 0:9900 .+
*MATCH*
```

SIG Data Policy Fallback

From Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco vManage Release 20.8.1, you can use the **sig-action fallback-to-routing** command to configure internet-bound traffic to be routed through the Cisco Catalyst SD-WAN overlay when all SIG tunnels are down. The following example shows the configuration of this fallback mechanism.

```
data-policy _VPN10_SIG_Fall_Back
  vpn-list VPN10
    sequence 1
     match
      app-list Google_Apps
      source-ip 0.0.0.0/0
     !
     action accept
      sig
      sig-action fallback-to-routing
     !
    !
  default-action drop
```

Ranking Color Preference Example

```
policy lists
  preferred-color-group GROUP1_COLORS
   primary-preference
    color-preference biz-internet
    path-preference direct-tunnel
   !
   secondary-preference
    color-preference mpls
    path-preference multi-hop-path
   !
   tertiary-preference
    color-preference lte
   !
  !
  preferred-color-group GROUP2_COLORS
   primary-preference
    color-preference mpls
   !
   secondary-preference
    color-preference biz-internet
   !
  !
  preferred-color-group GROUP3_COLORS
   primary-preference
    color-preference mpls biz-internet lte
   !
```

Data Policy for IPv6 Applications Example

```
policy
 data-policy _VPN1_Data-Policy-For-Ipv6-Traffic
  vpn-list VPN1
    sequence 1
     match
```

```
      app-list Msft-0365
      source-ipv6 0::0/0
      !
     action accept
     !
    !
  default-action drop
 !
 lists
  app-list Msft-0365
   app ms-office-web-apps
  !
  site-list SITE-100
   site-id 100
  !
  vpn-list VPN1
   vpn 1
  !
 !
!
apply-policy
 site-list SITE-100
  data-policy _VPN1_Data-Policy-For-Ipv6-Traffic all
 !
!
```