

Cisco Catalyst SD-WAN Application Intelligence Engine Flow

The topics in this section provide overview information about the Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) flow, and how to configure the flow using Cisco SD-WAN Manager or the CLI.

- Cisco Catalyst SD-WAN Application Intelligence Engine Flow Overview, on page 1
- Configure Cisco Catalyst SD-WAN Application Intelligence Engine Flow Using Cisco SD-WAN Manager, on page 2
- Configure SD-WAN Application Intelligence Engine Flow Using the CLI, on page 6
- Traffic Classification Using NBAR, on page 8

Cisco Catalyst SD-WAN Application Intelligence Engine Flow Overview

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

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

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

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

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

- Open Shortest Path First (OSPF)

- Border Gateway Protocol (BGP)
- Internet Control Message Protocol (ICMP)
- Bidirectional Forwarding Detection (BFD)

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

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

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

Apply Centralized Policy for SD-WAN Application Intelligence Engine Flow

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

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

To apply a centralized policy in the CLI:

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

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

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

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

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

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

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

Monitor Running Applications

To enable the SD-WAN Application Intelligence Engine (SAIE) infrastructure on Cisco vEdge devices, you must enable application visibility on the devices:



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

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

To display information about the running applications, use the **show app dpi supported-applications**, **show app dpi applications**, and **show app dpi flows** commands on the device.

View SAIE Applications

You can view the list of all the application-aware applications supported by the Cisco Catalyst SD-WAN software on the router using the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Click **WAN-Edge**, select the **Device** that supports the SD-WAN Application Intelligence Engine (SAIE) flow. The Cisco SD-WAN Manager Control Connections page is displayed.

3. In the left pane, select **Real Time** to view the device details.

4. From the **Device Options** drop-down, choose **SAIE Applications** to view the list of applications running on the device.

5. From the **Device Options** drop-down, choose **SAIE Supported Applications** to view the list of applications that are supported on the device.

Action Parameters for Configuring SD-WAN Application Intelligence Engine Flow

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

From the Cisco SD-WAN Manager menu, you can configure match parameters from:

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

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

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

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

Table 1:

Description	Cisco SD-WAN Manager	CLI Command	Value or Range
Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.	Click **Accept**.	**accept**	—
Count the accepted or dropped packets.	**Action Counter** Click **Accept**, then action **Counter**	**count** *counter-name*	Name of a counter. Use the **show policy access-lists counters** command on the Cisco device.
Discard the packet. This is the default action.	Click **Drop**	**drop**	—
Log the packet. Packets are placed into the messages and vsyslog system logging (syslog) files.	**Action Log** Click **Accept**, then **action Log**	**log**	To view the packet logs, use the **show app log flows** and **show log** commands.

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

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

Table 2:

Description	Cisco SD-WAN Manager	CLI Command	Value or Range
DSCP value.	Click **Accept**, then action **DSCP**.	**set dscp** *value*	0 through 63
Forwarding class.	Click **Accept**, then action **Forwarding Class**.	**set forwarding-class** *value*	Name of forwarding class
Direct matching packets to a TLOC that matches the color and encapsulation By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC.	Click **Accept**, then action **Local TLOC**.	**set local-tloc color** *color* [**encap** *encapsulation*]	*color* can be: **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green lte**, **metro-ethernet mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**. By default, *encapsulation* is **ipsec**. It can also be **gre**.
Direct matching packets to one of the TLOCs in the list if the TLOC matches the color and encapsulation By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the **restrict** option.	Click **Accept**, then action **Local TLOC**	**set local-tloc-list color** *color* **encap** *encapsulation* [**restrict**]	

Description	Cisco SD-WAN Manager	CLI Command	Value or Range
Set the next hop to which the packet should be forwarded.	Click **Accept**, then action **Next Hop**.	**set next-hop** *ip-address*	IP address
Apply a policer.	Click **Accept**, then action **Policer**.	**set policer** *policer-name*	Name of policer configured with a **policy policer** command.
Direct matching packets to the name service, before delivering the traffic to its ultimate destination. The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Configure the services themselves on the Cisco devices that are collocated with the service devices, using the **vpn service** configuration command.	Click **Accept**, then action **Service**.	**set service** *service-name* [**tloc** *ip-address* | **tloc-list** *list-name*] [**vpn** *vpn-id*]	Standard services: **FW**, **IDS**, **IDP** Custom services: **netsvc1**, **netsvc2**,**netsvc3**, **netsvc4** TLOC list is configured with a **policy lists tloc-list** list.
Direct matching packets to the named service that is reachable using a GRE tunnel whose source is in the transport VPN (VPN 0). If the GRE tunnel used to reach the service is down, packet routing falls back to using standard routing. To drop packets when a GRE tunnel to the service is unreachable, include the restrict option. In the service VPN, you must also advertise the service using the **service** command. You configure the GRE interface or interfaces in the transport VPN (VPN 0).	Click **Accept**, then action **Service**.	**set service** *service-name* [**tloc** *ip-address* | **tloc-list** *list-name*] [**vpn** *vpn-id*]	Standard services: **FW**, **IDS**, **IDP** Custom services: **netsvc1**, **netsvc2**,**netsvc3**, **netsvc4**
Direct traffic to a remote TLOC. The TLOC is defined by its IP address, color, and encapsulation.	Click **Accept**, then action **TLOC**.	**set local-tloc color** *color* [**encap** *encapsulation*]	TLOC address, color, and encapsulation
Direct traffic to one of the remote TLOCs in the TLOC list.	Click **Accept**, then action **TLOC**.	**set tloc-list** *list-name*	Name of a **policy lists tloc-list** list
Set the VPN that the packet is part of.	Click **Accept**, then action **VPN**.	**set vpn** *vpn-id*	Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.

Default Action

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

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

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

Configure SD-WAN Application Intelligence Engine Flow Using the CLI

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



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

1. Create a list of overlay network sites to which the data policy is to be applied using the **apply-policy** command:

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

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

   Create additional site lists, as needed.

2. Create lists of applications and application families that are to be subject to the data policy. Each list can contain one or more application names, or one or more application families. A single list cannot contain both applications and application families.

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

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

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

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

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

4. Create lists of TLOCs, as needed:

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

5. Define policing parameters, as needed:

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

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

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

7. Create a series of match–pair sequences:

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

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

8. Define match parameters based on applications:

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

9. Define additional match parameters for data packets:

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

10. Define actions to take when a match occurs:

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

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

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

12. Define additional actions to take.

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

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

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

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

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

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

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

- `show app dpi flows`

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

Traffic Classification Using NBAR

Table 3: Feature History

Feature	Release Information	Description
Traffic Classification Using NBAR	Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature extends Network-Based Application Recognition (NBAR) support to Cisco SD-WAN vEdge devices.

Information about NBAR

Starting from Cisco SD-WAN Release 20.6.1, Cisco vEdge devices use Network-Based Application Recognition as the SD-WAN Application Intelligence Engine (SAIE).

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

Cisco NBAR is a classification engine that recognizes and classifies a wide variety of protocols and applications. It performs the SAIE flow on network traffic to identify network applications according to their traffic characteristics.

The specific traffic characteristics of a network application are called an application signatures. Cisco packages the signature for an application, together with other information, as a protocol. Cisco packages a large set of protocols, covering numerous commonly occurring network applications, as a Protocol Pack. Cisco updates and distributes Protocol Packs regularly. They provide a database of network application signatures for NBAR to use to identify network application traffic.

The term network applications is defined broadly, and may include all of the following, and more:

- Social media websites
- Voice over IP (VoIP) applications
- Streaming audio and video, such as Cisco Webex
- Cloud applications, such as for cloud storage
- SaaS applications
- Custom network applications specific to an organization

Identifying applications is useful for monitoring network traffic, configuring application-aware traffic policy, and more.

To summarize network application signatures, protocols, and Protocol Packs, and how NBAR uses them:

- The traffic of a network application has unique characteristics that can be used to identify the traffic as belonging to that specific application. These characteristics are called application signatures.
- Cisco packages the signature for a specific network application as a protocol.
- Cisco packages a large set of protocols, covering commonly occurring internet applications, as Protocol Packs.
- Cisco NBAR performs deep packet inspection on traffic to gather the information required to identify the sources of the traffic, and uses protocols, such as those provided in Protocol Packs, to match that information to specific network applications. The result is that NBAR identifies the network applications producing traffic in the network.

Integration with NBAR

Upgrading the Cisco SD-WAN controllers and Cisco vEdge devices to Cisco SD-WAN Release 20.6.1 enables use of NBAR. The introduction of NBAR as the SD-WAN Application Intelligence Engine (SAIE) in this release may affect application-aware centralized policy. We recommend upgrading in the following order. For each step, see the notes regarding NBAR and application-aware policy.



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

1. Cisco vManage upgrade



Note During the upgrade to Cisco vManage Release 20.6.1, Cisco vManage indicates unsupported applications or any mappings that are missing in the configuration through a warning message. After the upgrade, when you log in, a dialog box displays the policy, app-list name, unsupported applications, and mappings that are missing in the app-list. You can download the information to review and modify the application-aware policies.

2. Cisco vSmart Controller and Cisco vBond Controller upgrade



Note The upgrade process for the Cisco SD-WAN controllers checks any existing application-aware centralized policies to determine whether they use applications not supported by NBAR. If so, the upgrade process prompts you with information about how to update the policies to be compatible with NBAR.

3. Cisco vEdge device upgrade

Note After the upgrade to Cisco SD-WAN Release 20.6.1, Cisco vEdge devices use NBAR for the SAIE flow. The application IDs in the cFlowd records are exported to external collectors from Cisco vEdge device. The application IDs correspond to NBAR and maps to application names accordingly. Application ID to application name mapping is available in NBAR Protocol Pack or in Cisco vEdge device show command, **show app dpi supported-applications app-id**.

For information about upgrading the software and best practices, see Upgrade the Software.

In Cisco vManage, you can configure policy using one of the following two methods:

1. Policy builder: You can choose the required applications from a list of supported applications to use in a policy. Cisco vManage maps these application names to the applications that are compatible with NBAR and generates SAIE-compatible application names.
2. Templates: With policy and device CLI templates, you can create custom policies that can include names of applications that are specific to SAIE.

When you upgrade Cisco vSmart Controller and push any policies or templates, the device generates syslogs, SNMP traps, and Netconf notifications for any application mismatch. You can view the notifications on the **Monitor** > **Events** page. The notification message lists the application names and the renamed application names.

You can view the alarms related to unsupported applications and the applications that need renaming on the **Monitor** > **Alarms** page. The alarm message lists the unsupported application names.

You can view the applications specified by application-aware policies using the `show app dpi applications` command. For information about this command, see show app dpi applications.

Supported Platforms for Traffic Classification Using NBAR

The following is a list of Cisco vEdge devices that support NBAR:

- vEdge 100b
- vEdge 100m
- vEdge 1000
- vEdge 2000
- vEdge 5000
- vEdge Cloud Router
- ISR1100- 4G
- ISR1100- 6G

Benefits of Using NBAR

- Consistent application classification behavior across Cisco SD-WAN platforms and mixed deployments.
- Access to all NBAR supported applications through Cisco vManage.

- Better performance and throughput with NBAR.
- NBAR supports better sub-classification for enterprise grade applications.

Restrictions for Traffic Classification Using NBAR

- The following features are not supported on Cisco vEdge devices in Cisco SD-WAN Release 20.6.1:
  - Custom Applications
  - Cisco Software-Defined Application Visibility and Control (SD-AVC)



Note These features also were not supported on Cisco vEdge devices in earlier releases.

- Cisco vManage displays alarms on the **Monitor** > **Alarms** page for custom applications to indicate that Cisco vEdge devices do not support custom applications.