Application Intelligence Engine Flow

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

SAIE flow overview

The SD-WAN Application Intelligence Engine (SAIE) flow is a packet inspection capability that

- looks into the packet past the basic header information to determine packet contents
- records packet information for statistical purposes or performs actions on the packet, and
- provides increased visibility into network traffic for understanding usage patterns and correlating network performance information.

SAIE flow benefits and configuration

Note In Cisco SD-WAN 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 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)

SAIE flow configuration using Cisco SD-WAN Manager

A SAIE flow configuration using Cisco SD-WAN Manager is a policy configuration process that

- guides you through creating and editing SD-WAN Application Intelligence Engine (SAIE) flow policy components,
- uses the Cisco SD-WAN Manager policy configuration wizard with sequential screens, and
- applies policies to sites and VPNs in the overlay network.

Configuration wizard screens

The wizard consists of the following sequential screens:

- 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 SAIE flow

Apply a centralized data policy for the SAIE flow to ensure it takes effect across specified sites in the overlay network.

A centralized data policy for the SAIE flow must be applied to a list of sites in the overlay network to ensure proper enforcement. The policy can be applied using either Cisco SD-WAN Manager or the CLI interface.

Procedure

Step 1 Choose your preferred method to apply the centralized policy.

- To apply a centralized policy in Cisco SD-WAN Manager, see *Configure Centralized Policy Using Cisco SD-WAN Manager*.
- To apply a centralized policy using the CLI, continue with the next step.

Step 2 Apply the data policy using the CLI command.

Example:

```
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.

The centralized data policy for the SAIE flow is successfully applied to the specified sites and is actively enforcing policy rules on data traffic passing through the network.

Monitor running applications

Enable the SAIE infrastructure to gain visibility into application traffic and monitor running applications on your network devices.

Application visibility is required to enable the Service Assurance and Insights Engine (SAIE) infrastructure on Cisco vEdge devices for monitoring network applications.

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

Before you begin

Follow these steps to monitor running applications:

Procedure

Step 1 Enable application visibility on the device.

Example:

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

Step 2 Display information about the running applications using the appropriate show commands.

Use the **show app DPI supported-applications**, **show app DPI applications**, and **show app DPI flows** commands on the device.

Application visibility is enabled on the device, and you can view information about supported applications, active applications, and application flows using the show commands.

View SAIE applications

This task allows you to view the list of all application-aware applications supported by the Cisco SD-WAN Manager software on the router.

Use this task to monitor and review SAIE applications running on your SD-WAN devices through the Cisco SD-WAN Manager interface.

Procedure

Step 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**.

Step 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.

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

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

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

You can now view the SAIE applications running on the selected device and the list of supported applications.

Action parameters for configuring SAIE 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.

Configuration access

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.

Basic action parameters

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

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**	—

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

Parameters for accepted packets

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

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** *name*	Text
Next hop. Specify the IP address of the next-hop router for traffic that matches the match criteria. The next-hop router must be directly connected to the local router.	Click **Accept**, then action **Next Hop**.	**set next-hop** *IP-address*	IP address
Policer. Limit the bandwidth used by the traffic flow.	Click **Accept**, then action **Policer**.	**set policer** *name*	Name of a policer configured using the **policy policer** command
Traffic-engineering path. Specify a path for the traffic to follow. The traffic is placed in a traffic-engineering tunnel.	Click **Accept**, then action **Traffic Engineering**.	**set traffic-engineering path** *name*	Name of a traffic-engineering path configured with the **policy traffic-engineering path** command
VPN. Redirect matching traffic to a specific VPN. The redirected traffic is routed to the VPN based on the VPN's route table.	Click **Accept**, then action **VPN**.	**set VPN** *VPN-id*	0 through 65530

Default action

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

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

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

Configure SAIE using the CLI

This task enables you to configure a centralized data policy for the SD-WAN Application Intelligence Engine (SAIE) flow to control application traffic behavior across overlay network sites.

The SAIE flow provides application intelligence and traffic control capabilities in SD-WAN deployments. Use this configuration when you need to implement centralized policies for application traffic management across multiple sites.

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

Follow these steps to configure a centralized data policy for the SD-WAN Application Intelligence Engine (SAIE) flow:

Procedure

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

Example:

```
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.

Step 2 Create lists of applications and application families that are to be subject to the data policy:

Example:

```
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
```

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.

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

Example:

```
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
```

Step 4 Create lists of TLOCs, as needed:

Example:

```
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]
```

Step 5 Define policing parameters, as needed:

Example:

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

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

Example:

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

Step 7 Create a series of match–pair sequences:

Example:

```
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).

Step 8 Define match parameters based on applications:

Example:

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

Step 9 Define additional match parameters for data packets:

Example:

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

Step 10 Define actions to take when a match occurs:

Example:

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

Step 11 For packets that are accepted, define the actions to take:

Example:

```
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]
```

Step 12 Apply the data policy to one or more sites:

Example:

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

What to do next

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`