Traffic Flow Monitoring with Cflowd

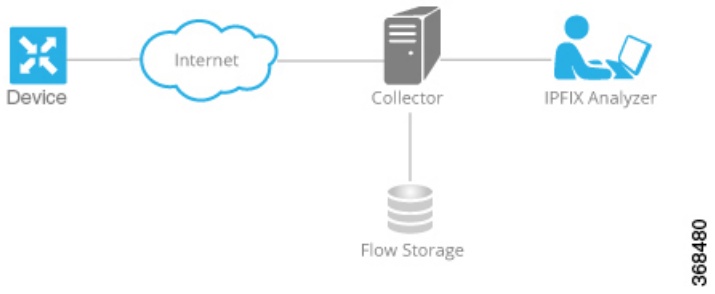
Cflowd monitors traffic flowing through Cisco IOS XE SD-WAN devices in the overlay network and exports flow information to a collector, where it can be processed by an IPFIX analyzer. For a traffic flow, cflowd periodically sends template reports to flow collector. These reports contain information about the flows and the data is extracted from the payload of these reports.

You can create a cflowd-template that defines the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the template is sent to the collectors (on Cisco vSmart Controllers only). You can configure a maximum of four cflowd collectors per Cisco IOS XE SD-WAN device. To have a cflowd-template take effect, apply it with the appropriate data policy.

You must configure at least one cflowd-template, but it need not contain any parameters. With no parameters, the data flow cache on the nodes is managed using default settings, and no flow export occurs.

Cflowd traffic flow monitoring is equivalent to Flexible Netflow (FNF).

The cflowd software implements cflowd version 10, as specified in *RFC 7011* and *RFC 7012*. Cflowd version 10 is also called the IP Flow Information Export (IPFIX) protocol.



Cflowd performs 1:1 sampling. Information about all flows is aggregated in the cflowd records; flows are not sampled. Cisco IOS XE SD-WAN devices do not cache any of the records that are exported to a collector.

Cisco IOS XE SD-WAN device IPFIX Information Elements Exported to the Collector

The Cisco IOS XE SD-WAN device cflowd software exports the following IPFIX information elements to the cflowd collector. Fields vary depending on the release that you are on. Common fields are exported to Cisco vManage and external exporters. Feature fields are exported only to Cisco vManage.

Before Cisco XE SD-WAN Release 17.2, Flexible NetFlow (FNF) exports all fields to external collectors and vManage. Starting from Cisco XE SD-WAN Release 17.2, FNF export the elements (that are marked

yes) in the following table to both external collectors and vManage. Other fields like “drop cause id” are for specific features and these fields are exported only to vManage, but not to external collector.

Information Element	Element ID	Exported to External Collector	Description	Data Type	Data Type Semantics	Units or Range
sourceIPv4Address	8	Yes	IPv4 source address in the IP packet header.	ipv4Address (4 bytes)	default	—
destinationIPv4Address	12	Yes	IPv4 destination address in the IP packet header.	IPv4Address (4 bytes)	default	—
ingressInterface	10	Yes	Index of the IP interface where packets of this flow are being received.	unsigned32 (4 bytes)	identifier	—
ipDiffServCodePoint	195	Yes	Value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field. This field spans the most significant 6 bits of the IPv4 TOS field.	unsigned8 (1 byte)	identifier	0 through 63
protocolIdentifier	4	Yes	Value of the protocol number in the Protocol field of the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.	unsigned8 (1 byte)	identifier	—
sourceTransportPort	7	Yes	Source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header. For GRE and IPsec flows, the value of this field is 0.	unsigned16 (2 bytes)	identifier	—
destinationTransportPort	11	Yes	Destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.	unsigned16 (2 bytes)	identifier	—
tcpControlBits	6	Yes	TCP control bits observed for the packets of this flow. This information is encoded as a bit field; each TCP control bit has a bit in this set. The bit is set to 1 if any observed packet of this flow has the corresponding TCP control bit set to 1. Otherwise, the bit is set to 0. For values of this field, see the *IANA IPFIX web page*.	unsigned8 (1 byte)	identifier	—

Information Element	Element ID	Exported to External Collector	Description	Data Type	Data Type Semantics	Units or Range
flowEndReason	136	Yes	Reason for the flow termination. For values of this field, see the *IANA IPFIX web page*.	unsigned8 (1 byte)	identifier	—
ingressoverlaysessionid	12432	Yes	A 32-bit identifier for input overlay session id.	unsigned32 (4 bytes)	identifier	—
VPN Identifier	Enterprise specific	Yes	Cisco IOS XE SD-WAN device VPN identifier. The device uses the enterprise ID for VIP_IANA_ENUM or 41916, and the VPN element ID is 4321.	unsigned32 (4 bytes)	identifier	0 through 65535
connection id long	12441	Yes	A 64-bit identifier for a connection between client and server.	Unsigned64 (8 bytes)	identifier	—
application id	95	Yes	A 32 bit identifier for an application name	unsigned32 (4 bytes)	identifier	—
egressInterface	14	Yes	Index of the IP interface where packets of this flow are being sent.	unsigned32 (4 bytes)	default	—
egressoverlaysessionid	12433	Yes	A 32-bit identifier for output overlay session id.	unsigned32 (4 bytes)	identifier	—
sdwan qos-queue-id	12446	No	Queue index for QoS.	unsigned8 (1 byte)	identifier	—
drop cause id	12442	No	A 16-bit identifier for a drop cause name.	unsigned16 (2 bytes)	identifier	—
counter bytes sdwan dropped long	12443	No	Total number of dropped octets in incoming packets for this flow at the observation point since initialization or re-initialization of the metering process for the observation point. The count includes the IP heads and the IP payload.	unsigned64 (8 bytes)	totalCounter	Octets
sdwan sla-not-met	12444	No	A Boolean to indicate if required SLA is met or not.	unsigned8 (1 byte)	identifier	—
sdwan preferred-color-not-met	12445	No	A Boolean to indicate if preferred color is met or not.	unsigned8 (1 byte)	identifier	—
counter packets sdwan dropped long	42329	No	Total number of dropped packets in incoming packets for this flow at the observation point since initialization or re-initialization of the metering process for the observation point.	unsigned64 (8 bytes)	totalCounter	Packets

Information Element	Element ID	Exported to External Collector	Description	Data Type	Data Type Semantics	Units or Range
octetDeltaCount	1	Yes	Number of octets since the previous report in incoming packets for this flow at the observation point. This number includes IP headers and IP payload.	unsigned64 (8 bytes)	deltaCounter	Octets
packetDeltaCount	2	Yes	Number of incoming packets since the previous report for this flow at this observation point.	unsigned64 (8 bytes)	deltaCounter	Packets
flowStartMilliseconds	152	Yes	Absolute timestamp of the first packet of this flow.	dateTime-MilliSeconds (8 bytes)	—	—
flowEndMilliseconds	153	Yes	Absolute timestamp of the last packet of this flow.	dateTime-MilliSeconds (8 bytes)	—	—

Configure Traffic Flow Monitoring on Cisco XE SD-WAN Devices

This topic provides the procedure for configuring cflowd traffic flow monitoring on Cisco IOS XE SD-WAN devices. Cflowd traffic flow monitoring uses Flexible Netflow (FNF) to export traffic data. To configure cflowd monitoring, follow these steps:

1. Configure global flow visibility.
2. Configure cflowd monitoring policy.

Configure Global Flow Visibility

To enable cflowd visibility globally on all Cisco IOS XE SD-WAN devices so that you can perform traffic flowing monitoring on traffic coming to the router from all VPNs in the LAN.

In Cisco vManage NMS

1. Select the **Configuration** > **Policies** screen.
2. Select the **Localized Policy** tab.
3. Click **Add Policy**.
4. Click **Next** to display the Configure Policy Setting screen.

5. Click **Netflow**.

From the CLI

```
Device# config-transaction
Device(config)# policy flow-visibility
Device(config-policy)# commit
Commit complete.
Device(config-policy)# end
Device#
```

Note The **policy app-visibility** command also enables global flow visibility by enabling **nbar** to get the application name.

Configure Global Application Visibility

To enable cflowd visibility globally on all Cisco IOS XE SD-WAN devices so that you can perform traffic flowing monitoring on traffic coming to the router from all VPNs in the LAN.

The difference between **flow-visibility** and **app-visibility** is that **app-visibility** enables **nbar** to see each application of the flows coming to the router from all VPNs in the LAN.

In Cisco vManage NMS

1. Select the **Configuration** > **Policies** screen.
2. Select the **Localized Policy** tab.
3. Click **Add Policy**.
4. Click **Next** to display the Configure Policy Setting screen.
5. Click **Application**.

From the CLI

```
Device# config-transaction
Device(config)# policy app-visibility
Device(config-policy)# commit
Commit complete.
Device(config-policy)# end
Device#
```

Configure Cflowd Monitoring Policy

To configure policy for cflowd traffic flow monitoring, use the Cisco vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

1. 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.
2. Configure Topology—Create the network structure to which the policy applies.

3. Configure Traffic Rules—Create the match and action conditions of a policy.
4. Apply Policies to Sites and VPNs—Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, you are creating policy components or blocks. In the last screen, you are applying policy blocks to sites and VPNs in the overlay network. For the cflowd policy to take effect, you must activate the policy.

For details of the Cisco vManage configuration procedure, see *Configuring Cflowd Traffic Flow Monitoring*.

From the CLI on the Cisco vSmart Controller that is controlling the Cisco IOS XE SD-WAN device:

1. Configure a cflowd template to specify flow visibility and flow sampling parameters:

```
vSmart(config)# policy cflowd-template template-name
vSmart(config-cflowd-template)#  flow-active-timeout seconds
vSmart(config-cflowd-template)#  flow-inactive-timeout seconds
vSmart(config-cflowd-template)#  flow-sampling-interval number
vSmart(config-cflowd-template)#  template-refresh seconds
```

2. Configure a flow collector:

```
vSmart(config-cflowd-template)# collector vpn vpn-id address
ip-address port port-number transport transport-type
source-interface interface-name
```

Note Cisco IOS XE SD-WAN devices only support UDP collector. Irrespective of which transport protocol is configured, the collector functionality on Cisco IOS XE SD-WAN device is always UDP.

3. Configure a data policy that defines traffic match parameters and that includes the action **cflowd**:

```
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy)# sequence number
vSmart(config-sequence)# match match-parameters
vSmart(config-sequence)# action cflowd
vSmart(config-data-policy)# default-action accept
```

4. Create lists of sites in the overlay network that contain the Cisco IOS XE SD-WAN devices to which you want to apply the traffic flow monitoring policy. To include multiple site in the list, configure multiple **vpn** *vpn-id* commands.

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

5. Apply the data policy to the sites in the overlay network that contain the Cisco IOS XE SD-WAN devices:

```
vSmart(config)# apply-policy site-list list-name
vSmart(config-site-list)# data-policy policy-name
vSmart(config-site-list)# cflowd-template template-name
```

Display Cflowd Information

To display cflowd information, use the following commands on the Cisco IOS XE SD-WAN device.

- show sdwan app-fwd cflowd collector

- show sdwan app-fwd cflowd flow-count
- show sdwan app-fwd cflowd flows [vpn *vpn-id*] format table
- show sdwan app-fwd cflowd statistics
- show sdwan app-fwd cflowd template [name *template-name*]
- show sdwan app-fwd cflowd flows format table

Configure Cflowd Traffic Flow Monitoring Using CLI

Following are the high-level steps for configuring a cflowd centralized data policy to perform traffic monitoring and to export traffic flows to a collector:

1. Create a list of overlay network sites to which the cflowd centralized data 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 a list of VPN for which the cflowd centralized data policy is to be configured (in the **policy data-policy** command):

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

3. Create lists of IP prefixes, as needed:

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

4. Configure a cflowd template, and optionally, configure template parameters, including the location of the cflowd collector, the flow export timers, and the flow sampling interval:

   ```
   vSmart(config)# policy cflowd-template template-name
   vSmart(config-cflowd-template-template-name)# collector vpn vpn-id address ip-address
    port port-number transport-type (transport_tcp | transport_udp) source-interface
   interface-name
   vSmart(config-cflowd-template-template-name)# flow-active-timeout seconds
   vSmart(config-cflowd-template-template-name)# flow-inactive-timeout seconds
   vSmart(config-cflowd-template-template-name)# template-refresh seconds
   ```

   ```
   vSmart(config)# policy cflowd-template cflowd_server
     flow-active-timeout   60
     flow-inactive-timeout 30
     template-refresh      80
   ```

   You must configure a cflowd template, but it need not contain any parameters. With no parameters, the data flow cache on router is managed using default settings, and no flow export occurs. You can configure one cflowd template per router, and it can export to a maximum of four collectors.

By default, an actively flowing data set is exported to the collector every 600 seconds (10 minutes), a data set for a flow on which no traffic is flowing is sent every 60 seconds (1 minute), and the cflowd template record fields (the three timer values) are sent to the collector every 90 seconds.

Also by default, a new flow is created immediately after an existing flow has ended. If you modify the configuration of the template record fields, the changes take effect only on flows that are created after the configuration change has been propagated to the router. Because an existing flow continues indefinitely, to have configuration changes take effect, clear the flow with the **clear app cflowd flows** command.

Note On Cisco IOS XE SD-WAN devices, flow-active-timeout is fixed as 60 seconds. If a flow-inactive-timeout is fixed as 10 seconds, it cannot be configured.

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 sequence to contain a single match–action pair:

```
vSmart(config-vpn-list-list-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. If no match occurs, the default action is taken.

7. Define match parameters for the data packets:

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

8. In the action, enable cflowd:

```
vSmart(config-sequence-number)# action cflowd
```

9. In the action, count or log data packets:

```
vSmart(config-sequence-number)# action count counter-name
vSmart(config-sequence-number)# action log
```

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

11. 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
```

12. Apply the policy and the cflowd template to one or more sites in the overlay network:

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name
vSmart(config)# apply-policy site-list list-name cflowd-template template-name
```

Structural Components of Policy Configuration for Cflowd

Here are the structural components required to configure cflowd on a Cisco vSmart Controller. Each component is explained in more detail in the sections below.

```
policy
  lists
    prefix-list list-name
      ip-prefix prefix
    site-list list-name
      site-id site-id
    vpn-list list-name
      vpn vpn-id
  log-frequency number
  cflowd-template template-name
    collector vpn vpn-id address ip-address port port-number transport transport-type
source-interface interface-name
    flow-active-timeout seconds
    flow-inactive-timeout seconds
    flow-sampling-interval number
    template-refresh seconds
  data-policy policy-name
    vpn-list list-name
      sequence number
        match
          match-parameters
         action
          cflowd
          count counter-name
          drop
          log
       default-action
         (accept | drop)
apply-policy site-list list-name
  data-policy policy-name
  cflowd-template template-name
```

Lists

Centralized data policy uses the following types of lists to group related items. You configure lists under the **policy lists** command hierarchy on Cisco vSmart Controllers.

Table 1:

List Type	Description	Command
Data prefixes	List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.	**data-prefix-list** list-name **ip-prefix** prefix/length
Sites	List of one or more site identifiers in the overlay network. To configure multiple sites in a single list, include multiple **site-id** options, specifying one site number in each option. You can specify a single site identifier (such as **site-id 1**) or a range of site identifiers (such as **site-id 1-10**).	**site-list** *list-name* **site-id** *site-id*
VPNs	List of one or more VPNs in the overlay network. To configure multiple VPNs in a single list, include multiple **vpn** options, specifying one VPN number in each option. You can specify a single VPN identifier (such as **vpn 1**) or a range of VPN identifiers (such as **vpn 1-10**).	**vpn-list** *list-name* **vpn** *vpn-id*

Cflowd Templates

For each cflowd data policy, you must create a template that defines the location of the flow collector:

```
vSmart(config)# policy cflowd-template template-name
```

The template can specify cflowd parameters or it can be empty. With no parameters, the data flow cache on vEdge nodes is managed using default settings, and no flow export occurs.

In the cflowd template, you can define the location of the flow collection:

```
vSmart# (config-cflowd-template-template-name)
vSamrt# collector vpn vpn-id address
ip-address port port-number
transport transport-type source-interface
interface-name
```

You can configure one cflowd template per Cisco vEdge device, and it can export to a maximum of four collectors.

You can configure flow export timers:

```
vSmart(config)# policy cflowd-template template-name
vSmart(config-cflowd-template-template-name)# flow-active-timeout seconds
vSmart(config-cflowd-template-template-name)# flow-inactive-timeout seconds
vSmart(config-cflowd-template-template-name)# template-refresh seconds
```

By default, an actively flowing data set is exported to the collector every 600 seconds (10 minutes), a data set for a flow on which no traffic is flowing is sent every 60 seconds (1 minute), and the cflowd template record fields are sent to the collector every 90 seconds. For flow sampling, by default, a new flow is started immediately after an existing flow ends.

For a single Cisco IOS XE SD-WAN device, you can configure a maximum of four collectors.

Data Policy Instance

For each centralized data policy, you create a named container for that policy with a **policy data-policy** *policy-name* command. For a single Cisco IOS XE SD-WAN device, you can configure a maximum of four cflowd policies.

VPN Lists

Each centralized data policy instance applies to the VPNs contained in a VPN list. Within the policy, you specify the VPN list with the **policy data-policy vpn-list** *list-name* command. The list name must be one that you created with a **policy lists vpn-list** *list-name* command.

Sequences

Within each VPN list, a centralized data policy contains sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy. You configure sequences with the **policy data-policy vpn-list sequence** command.

Each sequence in a centralized data policy can contain one **match** command and one **action** command.

Match Parameters

Centralized data policy can match IP prefixes and fields in the IP headers. You configure the match parameters under the **policy data-policy vpn-list sequence match** command.

For data policy, you can match these parameters:

Table 2:

Description	Command	Value or Range
Group of destination prefixes	**destination-data-prefix-list** *list-name*	Name of a **data-prefix-list** list.
Individual destination prefix	**destination-ip** *prefix*/*length*	IP prefix and prefix length
Destination port number	**destination-port** *number*	0 through 65535
DSCP value	**dscp** *number*	0 through 63
Internet Protocol number	**protocol** *number*	0 through 255
Group of source prefixes	**source-data-prefix-list** *list-name*	Name of a **data-prefix-list** list
Individual source prefix	**source-ip** *prefix*/*length*	IP prefix and prefix length
Source port number	**source-port** *address*	0 through 255

Action Parameters

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or rejected, and you can configure a counter for the accepted or rejected packets. You configure the action parameters under the **policy data-policy vpn-list sequence action** command.

Table 3:

Description	Command	Value or Range
Count the accepted or dropped packets.	**count** *counter-name*	Name of a counter. To display counter information, use the **show policy access-lists counters** command on the Cisco vEdge device.
Enable cflowd.	**cflowd**	—

For a packet that is accepted, configure the parameter **cflowd** to enable packet collection.

Default Action

If a data packet being evaluated does not match any of the match conditions in a control policy, a default action is applied to this route. By default, the route is rejected. To modify this behavior, include the **policy data-policy vpn-list default-action accept** command.

Apply and Enable Cflowd Policy

For a centralized data policy to take effect, you must apply it to a list of sites in the overlay network:

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name
```

To activate the cflowd template, associate it with the data policy:

```
vSmart(config)# apply-policy cflowd-template template-name
```

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

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

- Application-aware routing policy (**app-route-policy**)
- Centralized control policy (**control-policy**)
- Centralized data policy (**data-policy**)

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

As soon as you successfully activate the configuration by issuing a **commit** command, the Cisco vSmart Controller pushes the data policy to the Cisco IOS XE SD-WAN devices located in the specified sites. To view the policy as configured on the Cisco vSmart Controller, use the **show running-config** command on the Cisco vSmart Controller. To view the policy that has been pushed to the device, use the **show policy from-vsmart** command on the device.

To display the centralized data policy as configured on the Cisco vSmart Controller, use the **show running-config** command:

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

To display the centralized data policy that has been pushed to the Cisco IOS XE SD-WAN device, issue the **show omp data-policy** command on the device:

```
Device# show sdwan policy from-vsmart
```

Enable Cflowd Visibility on Cisco IOS XE SD-WAN device Devices

You can enable cflowd visibility directly on Cisco IOS XE SD-WAN devices, without configuring a data policy, so that you can perform traffic flow monitoring on traffic coming to the router from all VPNs in the LAN. To do this, configure cflowd visiblity on the device:

```
Device(config)# policy flow-visibility
```

To monitor the applications, use the **show app cflowd flows** and **show app cflowd statistics** commands on the device.

Cflowd Traffic Flow Monitoring Configuration Example

This topic shows a straightforward example of configuring traffic flow monitoring.

Configuration Steps

You enable cflowd traffic monitoring with a centralized data policy, so all configuration is done on a Cisco vSmart Controller. The following example procedure monitors all TCP traffic, sending it to a single collector:

1. Create a cflowd template to define the location of the collector and to modify cflowd timers:

```
vsmart(config)# policy cflowd-template test-cflowd-template
vsmart(config-cflowd-template-test-cflowd-template)# collector vpn 1 address 172.16.155.15
 port 13322 transport transport_udp
vsmart(config-cflowd-template-test-cflowd-template)# flow-inactive-timeout 60
vsmart(config-cflowd-template-test-cflowd-template)# template-refresh 90
```

2. Create a list of VPNs whose traffic you want to monitor:

```
vsmart(config)# policy lists vpn-list vpn_1 vpn 1
```

3. Create a list of sites to apply the data policy to:

```
vsmart(config)# policy lists site-list cflowd-sites site-id 400,500,600
```

4. Configure the data policy itself:

```
vsmart(config)# policy data-policy test-cflowd-policy
vsmart(config-data-policy-test-cflowd-policy)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 1
vsmart(config-sequence-1)# match protocol 6
vsmart(config-match)# exit
vsmart(config-sequence-1)# action accept cflowd
vsmart(config-action)# exit
vsmart(config-sequence-1)# exit
vsmart(config-vpn-list-vpn_1)# default-action accept
```

5. Apply the policy and the cflowd template to sites in the overlay network:

```
vsmart(config)# apply-policy site-list cflowd-sites data-policy test-cflowd-policy
Device(config-site-list-cflowd-sites)# cflowd-template test-cflowd-template
```

6. Activate the data policy:

```
vsmart(config-site-list-cflowd-sites)# validate
Validation complete
vsmart(config-site-list-cflowd-sites)# commit
Commit complete.
vsmart(config-site-list-cflowd-sites)# exit configuration-mode
```

Full Example Configuration

Here is what the full example cflowd configuration looks like:

```
vsmart(config)# show configuration
apply-policy
 site-list cflowd-sites
  data-policy     test-cflowd-policy
  cflowd-template test-cflowd-template
 !
!
policy
 data-policy test-cflowd-policy
  vpn-list vpn_1
   sequence 1
    match
     protocol 6
    !
    action accept
     cflowd
    !
   !
   default-action accept
  !
```

```
 !
 cflowd-template test-cflowd-template
  flow-inactive-timeout 60
  template-refresh      90
  collector vpn 1 address 192.0.2.1 port 13322 transport transport_udp
 !
 lists
  vpn-list vpn_1
   vpn 1
  !
  site-list cflowd-sites
   site-id 400,500,600
  !
 !
!
```

Check the Cflowd Configuration

After you activate the cflowd configuration on the Cisco vSmart Controller, you can check it with the **show running-config policy** and **show running-config apply-policy** commands on the Cisco vSmart Controller. In addition, the configuration is immediately pushed down to the Cisco IOS XE SD-WAN devices at the affected sites.

You can view the pushed cflowd template with the **show sdwan policy from-vsmart cflowd** command. Here is the output from a device at site 500:

```
Device# show sdwan policy from-vsmart cflowd-template
from-vsmart cflowd-template test-cflowd-template
 flow-active-timeout   30
 flow-inactive-timeout 60
 template-refresh      90
 collector vpn 1 address 192.0.2.1 port 13322 transport transport_udp
```

You can view all the pushed policy components with the **show sdwan policy from-vsmart** command:

```
Device# show sdwan policy from-vsmart
from-vsmart data-policy test-cflowd-policy
 vpn-list vpn_1
  sequence 1
   match
    protocol 6
   action accept
    cflowd
  default-action accept
from-vsmart cflowd-template test-cflowd-template
 flow-active-timeout   30
 flow-inactive-timeout 60
 template-refresh      90
 collector vpn 1 address 192.0.2.1 port 13322 transport transport_udp
from-vsmart lists vpn-list vpn_1
 vpn 1
```

Check the Flows

On the Cisco IOS XE SD-WAN devices affected by the cflowd data policy, various commands let you check the status of the cflowd flows.

```
Device# show sdwan app-fwd cflowd statistics

      data_packets             :      0
      template_packets         :      0
      total-packets            :      0
```

```
flow-refresh            :       123
flow-ageout             :       117
flow-end-detected       :       0
flow-end-forced         :       0
```