Configuring Cflowd Traffic Flow Monitoring

This article provides general procedures for configuring cflowd from the CLI.

Cflowd Configuration Components

Cflowd configuration is done using the basic components of centralized data policy. You configure cflowd template options, including the location of the cflowd collector (if you are sending the flow to a collector), and you must configure cflowd as an action in the data policy.

To create a centralized data policy that enables cflowd, you include the following components in the configuration on a vSmart controller:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match and action portions of the data policy configuration. For centralized data policy, you can group IP prefixes, sites, and VPNs.</td>
<td>policy lists</td>
</tr>
<tr>
<td>Cflowd template</td>
<td>Template that defines the location of cflowd collectors, how often sets of sampled flows should be sent to the collectors, and how often the cflowd template should be sent to the collectors. You must configure template, but it need not contain any parameters a collector is optional. With no parameters, the data flow cache on vEdge routers is managed using default settings, and no flow export occurs.</td>
<td>policy cflowd-template</td>
</tr>
<tr>
<td>Centralized data policy instance</td>
<td>Container for centralized data policy that filters packets based on IP prefix and IP packet header fields.</td>
<td>policy data-policy</td>
</tr>
<tr>
<td>VPN list</td>
<td>List of VPNs to which the data policy applies.</td>
<td>policy data-policy vpn-list</td>
</tr>
<tr>
<td>Numbered sequences of match–action pairs</td>
<td>Sequences that establish the order in which the policy components are applied</td>
<td>policy data-policy vpn-list sequence</td>
</tr>
<tr>
<td>Match parameters</td>
<td>Conditions that packets must match to be considered for a data policy.</td>
<td>policy data-policy vpn-</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>Configuration Command</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>list sequence match</td>
</tr>
<tr>
<td>Actions</td>
<td>Monitor traffic flow for matching packets.</td>
<td>policy data-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>list sequence match</td>
</tr>
<tr>
<td></td>
<td></td>
<td>action cflowd</td>
</tr>
<tr>
<td>Default action</td>
<td>Action to take if a packet matches none of the policy conditions.</td>
<td>policy data-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>list default-action</td>
</tr>
<tr>
<td>Application of centralized data policy</td>
<td>For a cflowd policy to take effect, you apply it to one or more sites in the overlay network, and you associated a cflowd template with the policy</td>
<td>apply-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>site-list data-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>apply-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>site-list cflowd-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>template</td>
</tr>
</tbody>
</table>

**General Configuration Procedure**

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 and the flow export timers:
   vSmart(config)# policy cflowd-template template-name
   vSmart(config-cflowd-template-template-name)# collector vpn vpn-id address ip-address port port-number transport (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

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

   You can configure one cflowd template per vEdge 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.

   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 vEdge router. Because an existing flow continues indefinitely, to have configuration changes take effect, clear the flow with the clear app cflowd flows command.

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 accept cflowd

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. If you want nonmatching prefixes to be accepted, configure the default action for the policy:
    vSmart(config-policy-name)# default-action accept

11. 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 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-id vpn-id
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
  template-refresh seconds

data-policy policy-name
  vpn-list list-name
  sequence number
  match
  match-parameters
  action
  accept cflowd
  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 vSmart controllers.

<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data prefix list</td>
<td>List of one or more IP prefixes.</td>
<td><code>data-prefix-list list-name</code> <code>ip-prefix prefix</code></td>
</tr>
<tr>
<td>Site list</td>
<td>List of one or more site identifiers in the overlay network. You can specify a single site identifier (such as <code>site-id 1</code>) or a range of site identifiers (such as <code>site-id 1-10</code>).</td>
<td><code>site-list list-name</code> <code>site-id site-id</code></td>
</tr>
<tr>
<td>VPN list</td>
<td>List of one or more VPNs in the overlay network. You can specify a single VPN identifier (such as <code>vpn-id 1</code>) or a range of VPN identifiers (such as <code>vpn-id 1-10</code>).</td>
<td><code>vpn-list list-name</code> <code>vpn vpn-id</code></td>
</tr>
</tbody>
</table>
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)# collector vpn vpn-id address ip-address port port-number transport transport-type source-interface interface-name
```

You can configure one cflowd template per vEdge router, 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 a single vEdge router, 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 vEdge router, 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>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group of destination prefixes.</td>
<td><code>destination-data-prefix-list list-name</code></td>
<td>Name of a <code>data-prefix-list</code> list.</td>
</tr>
<tr>
<td>Individual destination prefix.</td>
<td><code>destination-ip prefix/length</code></td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Destination port number.</td>
<td><code>destination-port number</code></td>
<td>0 through 65535</td>
</tr>
<tr>
<td>DSCP value.</td>
<td><code>dscp number</code></td>
<td>0 through 63</td>
</tr>
<tr>
<td>Internet Protocol number.</td>
<td><code>protocol number</code></td>
<td>0 through 255</td>
</tr>
<tr>
<td>Group of source prefixes.</td>
<td><code>source-data-prefix-list list-name</code></td>
<td>Name of a <code>data-prefix-list</code> list</td>
</tr>
<tr>
<td>Individual source prefix.</td>
<td><code>source-ip prefix/length</code></td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Source port number.</td>
<td><code>source-port address</code></td>
<td>0 through 255</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td><code>accept</code></td>
<td>—</td>
</tr>
<tr>
<td>Count the accepted or dropped packets</td>
<td><code>count counter-name</code></td>
<td>Name of a counter. Use the <code>show policy access-lists counter</code> command on the vEdge router to display counter information.</td>
</tr>
<tr>
<td>Description</td>
<td>Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>Discard the packet. This is the default action.</td>
<td>drop</td>
<td>—</td>
</tr>
</tbody>
</table>

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.

### Applying 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
```

While you can configure site lists that contain overlapping site IDs, when you apply more than one data policy, you must ensure that the site lists you apply the policies to have no overlapping site IDs. If you apply more than one data policy to the same site, one policy is applied and the other is ignored. However, the decision about which policy to apply is not under user control and so is not predictable. Which policy is applied is a function of the internal behavior of Viptela software when it processes the configuration. Therefore, you must design control policy carefully to ensure that more than one policy is not applied to the same site.

As soon as you successfully activate the configuration by issuing a `commit` command, the vSmart controller pushes the data policy to the vEdge routers located in the specified sites. To view the policy as configured on the vSmart controller, use the `show running-config` command on the vSmart controller. To view the policy that has been pushed to the vEdge router, use the `show policy from-vsmart` command on the vEdge router.

To display the centralized data policy as configured on the 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 vEdge router, issue the `show omp data-policy` command on the vEdge router:

```
vEdge# show policy from-vsmart
```
Enable Cflowd Visibility on vEdge Routers

You can enable cflowd visibility directly on vEdge routers, without configuring 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 visibility on the router:

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

To monitor the applications, use the `show app cflowd flows` and `show app cflowd statistics` commands on the vEdge router.

Additional Information

Cflowd Traffic Flow Monitoring Configuration Example
Traffic Flow Monitoring with Cflowd