

Chapter 27

Configuring Collector and Monitoring Services Interfaces

This chapter describes the following tasks:

Minimum Traffic Sampling Configuration on page 488

Configuring Flow Monitoring on page 489

Configuring Collector Interfaces on page 490

For detailed information about configuring flow monitoring and accounting services, see the *JUNOS Services Interfaces Configuration Guide*.



NOTE: Monitoring Services Physical Interface Cards (PICs) require Enhanced Flexible PIC Concentrators (FPCs).

Minimum Traffic Sampling Configuration

To configure traffic sampling on a logical interface, you must perform at least the following tasks:

Create a firewall filter to apply to the logical interfaces being sampled by including the filter statement at the [edit firewall family *family-name*] hierarchy level. In the filter then statement, you must specify the action modifier `sample` and the action `accept`.

```
[edit firewall family family-name]
filter filter-name {
  term term-name {
    then {
      sample;
      accept;
    }
  }
}
```

For more information about firewall filter actions and action modifiers, see the *JUNOS Policy Framework Configuration Guide*.

Another option is to configure the direction of traffic to be sampled by including the sampling statement at the [edit interfaces *interface-name* unit *logical-unit-number* family *inet*] hierarchy level, specifying `input`, `output`, or `both`.

```
[edit interfaces interface-name unit logical-unit-number family inet]
sampling {
  (input | output | input output);
}
```

Apply the filter to the interfaces on which you want to sample traffic by including the address and filter statements at the [edit interfaces *interface-name* unit *logical-unit-number* family *family-name*] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family family-name]
address address {
  destination address;
}
filter {
  input filter-name;
}
```

Enable sampling and specify a nonzero sampling rate by including the sampling statement at the [edit forwarding-options] hierarchy level:

```
[edit forwarding-options]
sampling {
  input {
    family inet {
      max-packets-per-second number;
      rate number;
    }
  }
}
```

Configuring Flow Monitoring

The flow-monitoring application performs traffic flow monitoring and enables lawful interception of traffic between two routing platforms. Traffic flows can either be passively monitored by an offline routing platform or actively monitored by a routing platform participating in the network.

To enable flow monitoring on the Monitoring Services PIC, include the following statements at the [edit interfaces] hierarchy level:

```
[edit interfaces]
mo-fpc/pic/port {
  unit logical-unit-number {
    family inet {
      address address {
        destination address;
      }
      filter {
        group filter-group-number;
        input filter-name;
        output filter-name;
      }
      sampling {
        (input | output | input output);
      }
    }
  }
  multiservice-options {
    boot-command filename;
    (core-dump | no-core-dump);
    (syslog | no-syslog);
  }
}
```

Specify the physical and logical location of the flow-monitoring interface. unit 0 is not available, because it is already used by internal processes. Specify the source and destination addresses. The filter statement allows you to associate an input or output filter or a filter group that you have already configured for this purpose. The sampling statement specifies the traffic direction, either input, output, or both.

The multiservice-options statement allows you to configure properties related to flow-monitoring interfaces:

Include the boot-command statement to specify a boot image for the Monitoring Services interface.

Include the core-dump statement to enable storage of core files in /var/tmp.

Include the syslog statement to enable storage of system logging information in /var/log.

To configure flow-monitoring properties, include the following statements at the [edit forwarding-options] hierarchy level:

```
[edit forwarding-options]
monitoring name;
family inet {
  output {
    cflowd hostname port port-number;
    export-format format;
    flow-active-timeout seconds;
    flow-inactive-timeout seconds;
    interface interface-name {
      engine-id number;
      engine-type number;
      input-interface-index number;
      output-interface-index number;
      source-address address;
    }
  }
}
```

For more information about flow-monitoring properties, see the *JUNOS Services Interfaces Configuration Guide*. For a more detailed configuration example, see the *JUNOS Feature Guide*.

Configuring Collector Interfaces

With a flow collector interface, you can process and export multiple cflowd records. The flow collector interface combines multiple cflowd records into a compressed ASCII data file and exports the file to an FTP server.

You configure a flow collector interface on the Monitoring Services II PIC. You can use a Monitoring Services II PIC for either flow collection or monitoring, but not both services simultaneously.

To convert the PIC to perform flow collection service, complete the following tasks:

1. Include the application flow-collector statements at the [edit chassis fpc *fpc-slot-number* pic *pic-slot-number* monitoring-services] hierarchy level:

```
[edit chassis fpc fpc-slot-number pic pic-slot-number monitoring-services]
application flow-collector;
```

2. Take the Monitoring Services II PIC offline and bring the PIC back online.

When the PIC is back online, all monitoring services interfaces (*mo-fpc/pic/port*) on the specified PIC are converted to collector interfaces (*cp-fpc/pic/port*).



NOTE: A flow collector interface, designated by the *cp-fpc/pic/port* interface name, requires three logical interfaces for correct operation. Units 0 and 1 are used to send the compressed ASCII data files to an FTP server. Unit 2 is used to receive cflowd records from a monitoring services interface.

Unlike conventional interfaces, the address statement at the [edit interfaces *cp-fpc/pic/port* unit *unit-number* family inet] hierarchy level corresponds to the IP address of the Routing Engine. Likewise, the destination statement at the [edit interfaces *cp-fpc/pic/port* unit *unit-number* family inet address *ip-address*] hierarchy level corresponds to the IP address of the flow collector interface. As a result, you must configure the destination statement for unit 0 and unit 1 with local addresses that can reach the FTP server. Similarly, configure the destination statement for unit 2 with a local IP address, so it can reach the monitoring services interface that sends cflowd records.

For more information about the application flow-collector statements, see the *JUNOS System Basics Configuration Guide*.

For detailed information about configuring the collector interface, see the *JUNOS Services Interfaces Configuration Guide* and the *JUNOS Feature Guide*.

