

# Chapter 24

## Configure Monitoring Services Interfaces

This chapter describes the following tasks for configuring traffic sampling and flow-monitoring properties:

Minimum Traffic Sampling Configuration on page 315

Configure Flow Monitoring on page 316

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

### 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 Internet Software Configuration Guide: Policy Framework*.

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;
}
```

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 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;
    }
  }
}
```

## Configure Flow Monitoring

The flow-monitoring application performs traffic flow monitoring and enables lawful interception of traffic between two routers. Traffic flows can either be passively monitored by an offline router or actively monitored by a router 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 ];
      }
    }
  }
  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 host-name {
        aggregation {
          autonomous-system;
          destination-prefix;
          protocol-port;
          source-destination-prefix {
            caida-compliant;
          }
          source-prefix;
        }
        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 Internet Software Configuration Guide: Services Interfaces*.

