Chapter 10
Configure Adaptive Services Interfaces

You can configure basic properties of the adaptive services interface on a global level, including default values for system logging, timeout, and intrusion detection properties. To configure properties for the entire interface, you include statements at the [edit interfaces] hierarchy level:

```
[edit]
interfaces interface-name {
    logical-unit-number {
        family inet {
            address address {
...
            }
            filter {
                input input-filter-name;
                output output-filter-name;
            }
            policer {
                input input-filter-name;
                output output-filter-name;
            }
            service {
                input {
                    [ service-set service-set-name <service-filter filter-name> ];
                    post-service-filter filter-name;
                }
                output {
                    [ service-set service-set-name <service-filter filter-name> ];
                }
            }
        service-domain (inside | outside);
    }
    service-options {
        inactivity-timeout seconds;
        open-timeout seconds;
        syslog {
            host host-name {
                facility-override facility-name;
                log-prefix prefix-number;
                [ services priority-level ];
            }
        }
    }
}
```

This chapter contains the following sections:

For detailed information about configuring the Adaptive Services PIC, see the *JUNOS Internet Software Configuration Guide: Services Interfaces*.

Configure Service Interface Properties

This section describes the following tasks for configuring service sets:

Configure the Interface Address and Domain

Just as you do for other network interfaces, you configure an IP address for a service interface by including the address statement at the [edit interfaces *interface-name* unit *logical-unit-number* family inet] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet]
address address {
...
}
```

Assign an IP address to the interface by configuring the *address* value. The GSP supports only IP4 addresses configured using the family inet statement.

For information on other addressing properties you can configure that are not specific to service interfaces, see “Configure the Interface Address” on page 81.

The service-domain statement specifies whether the interface is used within the network or to communicate with remote devices. The software uses this setting to determine which default stateful firewall rules to apply, and to determine the default direction for service rules. To configure, include the service-domain statement at the [edit interfaces *interface-name* unit *logical-unit-number*] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number]
service-domain (inside | outside);
```

Configure Default Timeout Settings

You can specify global default settings for certain timers that apply for the entire interface. There are two statements of this type:

inactivity-timeout—Sets the inactivity timeout period for established flows, after which they are no longer valid.

open-timeout—Sets the timeout period for TCP session establishment, for use with syn-cookie defenses against network intrusion.

To configure a setting for the inactivity timeout period, include the inactivity-timeout statement at the [edit interfaces *interface-name* service-options] hierarchy level:

```
[edit interfaces interface-name service-options]
inactivity-timeout seconds;
```

The default value is 30 seconds. The range of possible values is 4 through 65,535 seconds. Any value you configure in the application protocol definition at the [edit applications] hierarchy level overrides the value specified here.

To configure a setting for the TCP session establishment timeout period, include the open-timeout statement at the [edit interfaces *interface-name* service-options] hierarchy level:

```
[edit interfaces interface-name service-options]
open-timeout seconds;
```

The default value is 30 seconds. Any value you configure in the IDS service definition at the [edit services ids] hierarchy level overrides the value specified here.

Configure Default System Log Properties

You specify properties that control how system log messages are generated for the interface as a whole. If you configure different values for the same properties at the [edit services service-set *service-set-name*] hierarchy level, the service-set values override the values configured for the interface.

To configure interface-wide default system logging values, include the syslog statement at the [edit interfaces *interface-name* service-options] hierarchy level:

```
[edit interfaces interface-name service-options]
syslog {
    host host-name {
        facility-override facility-name;
        log-prefix prefix-number;
        [ services priority-level ];
    }
}
```

Configure the host statement with a hostname that specifies the system log target server. The hostname local directs system log messages to the Routing Engine.

You can configure one or more facilities with a specified priority level. The supported facilities are: any, authorization, change-log, conflict-log, cron, daemon, firewall, interactive-commands, kernel, pfe, and user. The valid priority settings are shown in Table 11 on page 114:

Table 11: System Log Priority Level Settings

Priority Level	Description
alert	Conditions that should be corrected immediately.
any	Matches any level.
critical	Critical conditions.
emergency	Panic conditions.
error	Error conditions.
info	Informational messages.
notice	Conditions that require special handling.
warning	Warning messages.

To use one particular facility code for all logging to the specified system log host, include the facility-override statement at the [edit interfaces *interface-name* service-options syslog host *host-name*] hierarchy level:

```
[edit interfaces interface-name service-options syslog host host-name]
facility-override facility-name;
```

To specify an address prefix for all logging to this system log host, include the log-prefix statement at the [edit interfaces *interface-name* service-options syslog host *host-name*] hierarchy level:

```
[edit interfaces interface-name service-options syslog host host-name]
log-prefix prefix-number;
```

Apply Filters and Services to an Interface

When you have defined and grouped the service rules by configuring the service-set definition, you need to apply services to one or more interfaces installed on the router To associate a defined service set with an interface, include the service-set statement at the [edit interfaces *interface-name* unit *logical-unit-number* family inet service (input | output)] hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet service]
input {
    [ service-set service-set-name <service-filter filter-name> ];
    post-service-filter filter-name;
}
output {
    [ service-set service-set-name <service-filter filter-name> ];
}
```

You can configure different service sets on the input and output sides of the interface. You can optionally include filters before or after each service set to refine the target and additionally process the traffic. For an example, see “Example: Configure a Service Interface” on page 115.

Example: Configure a Service Interface

The following example applies my-input-service-set on an interface-wide basis. All traffic that is accepted by my-input-filter has my-service-set applied to it. After the service set is applied, additional filtering is done using my-post-service-input-filter.

```
[edit interfaces fe-0/0/0]
unit 0 {
    family inet {
        filter {
            input my-input-filter;
            output my-output-filter;
        }
        service {
            input {
                service-set my-input-service-set;
                post-service-filter my-post-service-input-filter;
            }
            output {
                service-set my-output-service-set;
            }
        }
    }
}
```