

Chapter 18

Configure Service Sets

A *service set* is a collection of services to be performed on the Adaptive Services PIC (AS PIC). To configure service sets, you include the following statements at the [edit services] hierarchy level of the configuration:

```
[edit services]
service-set service-set-name {
  ([ ids-rules rule-names ] | ids-rule-sets rule-set-name);
  ([ ipsec-vpn-rules rule-names ] | ipsec-vpn-rule-sets rule-set-name);
  ([ nat-rules rule-names ] | nat-rule-sets rule-set-name);
  ([ stateful-firewall-rules rule-names ] | stateful-firewall-rule-sets rule-set-name);
  interface-service {
    service-interface interface-name;
  }
  ipsec-vpn-options {
    local-gateway address;
  }
  next-hop-service {
    inside-service-interface name.number;
    outside-service-interface name.number;
  }
  syslog {
    host hostname {
      services priority-level;
      facility-override facility-name;
      log-prefix prefix-number;
    }
  }
}
adaptive-services-pics {
  traceoptions {
    flag flag;
  }
}
```

This chapter contains the following sections:

Configure Service Set Properties on page 194

Apply a Service Set to an Interface on page 197

Trace Adaptive Services PIC Operations on page 198

Example: Configure Service Sets on page 199

Configure Service Set Properties

This section describes the following tasks for configuring service sets:

Configure Service Interfaces on page 194

Configure Service Rules on page 195

Configure System Log Properties on page 196

Configure Service Interfaces

You configure a *service interface* to specify the AS PIC interface on which the service is to be performed. You can configure two types of service sets, interface service and next-hop service, but you must configure each service set as one or the other:

Interface service— Service set to be used as an action modifier across an entire interface. When you apply the service set to an interface, it automatically ensures that packets are directed to the PIC. The service set retains the input-interface information even after services are applied, so that functions such as filter-class forwarding and DCU that depend on input-interface information continue to work.

To configure interface service, include the `interface-service` statement at the `[edit services service-set service-set-name]` hierarchy level:

```
[edit services service-set service-set-name]
interface-service {
    service-interface interface-name;
}
```

Configure the service interface associated with an interface-wide service set. Only the device name is needed, because the router software manages logical unit numbers automatically. The service interface must be an AS PIC interface for which you have configured unit 0 family inet at the `[edit interfaces interface-name]` hierarchy level.

Next-hop service—Service set to be used as a forwarding next hop. This is useful when services need to apply to an entire VRF or when routing decisions determine that services need to be performed. When configuring this type of service set, you must specify AS PIC units for inside the network and outside the network.

To configure next-hop service, include the `next-hop-service` statement at the `[edit services service-set service-set-name]` hierarchy level:

```
[edit services service-set service-set-name]
next-hop-service {
    inside-service-interface name.number;
    outside-service-interface name.number;
}
```

The values you configure for the `inside-service-interface` and `outside-service-interface` statements must correspond to the interface type setting you specify at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level:

`inside-service-interface` must be an AS PIC logical interface for which you have configured `service-domain inside` at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level. You cannot configure unit 0 for this purpose, and the logical interface you choose must not be used by another service set.

`outside-service-interface` must be an AS PIC logical interface for which you have configured `service-domain outside` at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level. You cannot configure unit 0 for this purpose, and the logical interface you choose must not be used by another service set.

The interfaces you specify with the `inside-service-interface` and `outside-service-interface` statements must be logical interfaces on the same AS PIC. For more information, see “Configure the Interface Address and Domain” on page 214.

You can use logical interfaces to preserve redundancy by specifying the interface designation with a period (.) and a number following it; for example:

```
sp-1/1/0.1
```

Configure Service Rules

You specify the collection of rules and rule sets that constitute the service set. The router performs rule sets in the order in which they appear in the configuration. You can include only one rule set for each service type. You configure the rule names and content for each service type at the `[edit services name]` hierarchy level for each type:

You configure intrusion detection rules at the `[edit services ids]` hierarchy level; for more information, see “Configure Intrusion Detection Services” on page 87.

You configure Internet Protocol Security (IPSec) rules at the `[edit services ipsec-vpn]` hierarchy level; for more information, see “Configure IPSec Services” on page 105.

You configure Network Address Translation rules at the `[edit services nat]` hierarchy level; for more information, see “Configure Network Address Translation Services” on page 69.

You configure stateful firewall rules at the `[edit services stateful-firewall]` hierarchy level; for more information, see “Configure Stateful Firewall Services” on page 57.

To configure the rules and rule sets that constitute a service set, include the following statements at the [edit services service-set *service-set-name*] hierarchy level:

```
[edit services service-set service-set-name]
([ ids-rules rule-names ] | ids-rule-sets rule-set-name);
([ ipsec-vpn-rules rule-names ] | ipsec-vpn-rule-sets rule-set-name);
([ nat-rules rule-names ] | nat-rule-sets rule-set-name);
([ stateful-firewall-rules rule-names ] | stateful-firewall-rule-sets rule-set-name);
```

For each service type, you can include one or more individual rules, or one rule set. If you include IDS or NAT rules, you must also include stateful firewall rules.

If you configure a service set with IPSec rules, it must not contain rules for any other services. You can, however, configure another service set containing rules for the other services and apply both service sets to the same interface.

If you configure an IPSec service set, you must also configure a local address by including the local-gateway statement at the [edit services service-set *service-set-name* ipsec-vpn-options] hierarchy level:

```
[edit services service-set service-set-name ipsec-vpn-options]
local-gateway address;
```

Configure System Log Properties

You specify properties that control how system log messages are generated for the service set. These values override the values configured at the [edit interfaces *interface-name* sp-options] hierarchy level.

To configure service-set-specific system logging values, include the syslog statement at the [edit services service-set *service-set-name*] hierarchy level:

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

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. The hostname must be included in inet.0. You can specify only one system log host.

You can configure a priority level for system logging messages generated by the service set. The valid priority settings are shown in Table 9.

Table 9: 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 services service-set *service-set-name* syslog host *hostname*] hierarchy level:

```
[edit services service-set service-set-name syslog host hostname]
  facility-override facility-name;
```

The supported facilities are: authorization, daemon, ftp, kernel, user, and local0 through local7.

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

```
[edit services service-set service-set-name syslog host hostname]
  log-prefix prefix-number;
```

Apply a Service Set 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 associated with each service set to refine the target and additionally process the traffic. If you include the `service-set` statement without a `service-filter` definition, the router software assumes the match condition is true and selects the service set for processing automatically.

You can also include more than one service set definition on each side of the interface. If you include multiple service sets, the router software evaluates them in the order in which they appear in the configuration. It executes the first service set for which it finds a match in the service filter and ignores the subsequent definitions.

An additional statement allows you to specify a filter for processing the traffic after the input service set is executed. To configure this type of filter, include the `post-service-filter` statement at the `[edit interfaces interface-name unit logical-unit-number family inet service input]` hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet service input]
post-service-filter filter-name;
```

For an example, see “Example: Configure Service Sets” on page 199.

Trace Adaptive Services PIC Operations

Tracing operations track all Adaptive Services PIC operations and record them in a log file in the `/var/log` directory. By default, this file is named `/var/log/spd`.

To trace AS PIC operations, include the `traceoptions` statement at the `[edit services adaptive-services-pics]` hierarchy level:

```
[edit services adaptive-services-pics]
traceoptions {
  flag flag;
}
```

You can specify the following AS PIC tracing flags:

- `all`—Trace everything.
- `configuration`—Trace configuration events.
- `routing-protocol`—Trace routing protocol events.
- `routing-socket`—Trace routing socket events.

Example: Configure Service Sets

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

```
[edit interfaces fe-0/1/0]
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;
      }
    }
  }
}
```

