ERICSSON

Configuring Service Policies

SYSTEM ADMINISTRATOR GUIDE

29/1543-CRA 119 1170/1-V1 Uen D

Contents

1	**Overview**	**1**
2	**Configuration and Operations Tasks**	**3**
2.1	Configure a Service Policy	3
2.2	Attach a Service Policy to Subscriber Sessions	3
2.3	Operations Tasks	4
3	**Configuration Examples**	**5**

1 Overview

This document provides an overview of the service policy features supported by the SmartEdge® router and describes the tasks used to configure, monitor, and administer these features. This document also provides configuration examples of service policy features.

Service policies determine the contexts that Point-to-Point Protocol (PPP) and PPP over Ethernet (PPPoE) subscribers can access by verifying the domain or context name associate with subscriber records. PPP and PPPoE sessions are established by an authentication, authorization, and accounting (AAA) process. Also, you can configure a service policy so that the AAA process blocks specified PPPoE contexts and domains.

A service policy can be attached to any PPP- or PPPoE-encapsulated circuit using the **`bind authentication`** command (in ATM PVC, dot1q PVC, port, and protocol configuration mode); for more information, see *Configuring Bindings*.

When the SmartEdge router is configured as a Layer 2 Tunneling Protocol (L2TP) network server (LNS), a service policy can be attached to subscriber sessions on the L2TP tunnel with the **`session-auth`** command (in L2TP peer configuration mode); for more information, see *Configuring L2TP*.

2 Configuration and Operations Tasks

To configure service policies, perform the tasks described in the following sections.

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see *Command List*.

2.1 Configure a Service Policy

To configure a service policy, perform the tasks described in Table 1.

Table 1 Configure a Service Policy

Task	Root Command	Notes
Configure a service policy name and access service policy configuration mode.	*service-policy*	Enter this command in global configuration mode.
Configure the domain or context to which subscribers are allowed access.	*allow*	Enter this command in service policy configuration mode. To specify more than one context or domain, use this command multiple times. Any context names that are not specified through this command are implicitly denied.
Configure the domain or context to which subscribers are denied access.	*deny (service policy)*	Enter this command in service policy configuration mode. To specify more than one context or domain, use this command multiple times. Any context names that are not specified in this command are implicitly allowed.

2.2 Attach a Service Policy to Subscriber Sessions

To attach a service policy to subscriber sessions, perform the appropriate task described in Table 2.

Table 2 Attach a Service Policy to Subscriber Sessions

Task	Root Command	Notes
Attach a service policy to PPP- and PPPoE-encapsulated subscriber sessions.	*bind authentication*	Enter this command in ATM PVC, dot1q PVC, port, and protocol configuration modes.
Attach a service policy to PPP-encapsulated subscriber sessions on L2TP tunnels.	*session-auth*	Enter this command in L2TP peer configuration mode.

2.3 Operations Tasks

To monitor, troubleshoot, and administer service policy features on the SmartEdge router, use the **`debug aaa authentication`** command in exec mode to display status messages when service policies are attached to subscriber sessions.

3 Configuration Examples

The following example configures the service policy, **local-only**, which allows subscribers access to the **local** context only. The service policy is applied to subscriber sessions using the specified Asynchronous Transfer Mode (ATM) permanent virtual circuit (PVC):

```
[local]Redback(config)#service-policy name local-only
[local]Redback(config-policy-svc)#allow context name local
[local]Redback(config-policy-svc)#exit
[local]Redback(config)#port atm 4/1
[local]Redback(config-atm-oc)#atm pvc 3 5 profile atm1 encapsulation ppp
[local]Redback(config-atm-pvc)#bind authentication pap service-policy local-only
```

The following example restricts all subscribers that originate their session on ATM PVC **0 32** to be tunneled only to the **corp1** remote peer:

```
[local]Redback(config)#service-policy Corp-One-Permit
[local]Redback(config-policy-svc)#allow corp1.com
[local]Redback(config-policy-svc)#exit
[local]Redback(config)#context corporations
[local]Redback(config-ctx)#aaa authentication subscriber none
[local]Redback(config-ctx)#domain corp1.com
[local]Redback(config-ctx)#domain corp2.com
[local]Redback(config-ctx)#domain corp3.com
[local]Redback(config-ctx)#l2tp-peer name corp1 media udp-ip remote dns corp1.com local 10.1.1.1
[local]Redback(config-l2tp)#domain corp1.com
[local]Redback(config-l2tp)#exit
[local]Redback(config-ctx)#l2tp-peer name corp2 media udp-ip remote dns corp2.com local 10.1.1.2
[local]Redback(config-l2tp)#domain corp2.com
[local]Redback(config-l2tp)#exit
[local]Redback(config-ctx)#l2tp-peer name corp3 media udp-ip remote dns corp3.com local 10.1.1.3
[local]Redback(config-l2tp)#domain corp3.com
[local]Redback(config-l2tp)#exit
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#tunnel domain
[local]Redback(config-sub)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#port atm 5/1
[local]Redback(config-atm)#atm pvc 0 32 profile atm-pro-1 encapsulation pppoe
[local]Redback(config-atm-pvc)#bind authentication service-policy Corp-One-Permit
```

The following example blocks all subscribers using the service policy **local-only** from establishing a successful PPPoE session to the context **ctx_black** and domain **dmn_black** from:

```
[local]Redback(config)#service-policy name local-only
[local]Redback(config-policy-svc)#deny context name ctx_black
[local]Redback(config-policy-svc)#deny domain name dmn_black
```

Once you have entered the above commands, you need to bind the settings to a circuit to put them into effect. The following example binds the **local-only** service policy to the **ubr1** ATM PVC profile:

```
[local]Redback(config)#port atm 11/1
[local]Redback(config-atm-ds3)#atm pvc 0 42 profile ubr1 encapsulation pppoe
[local]Redback(config-atm-ds3)#atm pvc 0 43 profile ubr1 encapsulation pppoe
[local]Redback(config-atm-pvc)#bind authentication pap service-policy local-only
```