Advanced Services Configuration and Operation Using the SmartEdge OS CLI

SYSTEM ADMINISTRATOR GUIDE

1/1543-CRA 119 1170/1-V1 Uen F

Copyright

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Introduction

The Advanced Services Engine (ASE) and the Advanced Services Engine 2 (ASE2) cards contain two Advanced Service Processors (ASPs) that provide additional processing power on a SmartEdge® router. ASE-based services (Security Service) run on these ASPs. In the current release of the SmartEdge OS, the ASE-based Security Service supports the following two applications:

- Internet Protocol Security (IPsec) Virtual Private Network (VPN), which provides support for secure tunnels.
- Application Traffic Management, which provides support for managing application traffic using Deep Packet Inspection (DPI) and heuristic mechanisms.

You can use the Command Line Interface (CLI) of the SmartEdge OS to configure these applications.

1.1 Scope

This document describes how to use the CLI to add an ASE or ASE2 card to the configuration of a SmartEdge router, and configure the ASP pools and ASP groups. ASP pools and groups distribute the processing capabilities of the ASPs on the ASE cards installed in the router, provide load balancing when multiple ASPs are installed, and support resiliency when excess ASPs are available. The document also describes how to view information about ASP pools and groups, and configure ASP logging.

1.2 Target Groups

This document is intended for network planners responsible for the design of advanced network services that use the SmartEdge router and for operators of the SmartEdge OS responsible for configuring individual SmartEdge routers.

1.3 Prerequisites

The contexts that carry traffic that you want directed to ASPs on an ASE card for processing by the security applications must be configured on the SmartEdge router. Until a context is associated with an ASP group, ASE based services cannot be accessed.

Before you configure ASP logging, a loopback interface must be configured in the local context for use as the ASP log source IP address. Its IP address is required to configure ASP logging. The IP address and port on the log server to which the ASP log messages are forwarded must also be known. The only supported transport protocol in this release is User Datagram Protocol (UDP).

2 ASE Card Provisioning

Provisioning the ASE card and the ASE2 card on a SmartEdge router prepares the ASPs on the card to provide ASE based services.

You can add an ASE card to the configuration of a SmartEdge router before it is physically installed in the chassis. The card is detected when it is physically installed and the ASE configuration is processed. It takes longer for an ASE card to become active and start processing traffic than a traffic card due to the additional complexity of the ASE based services provided by the ASPs on the card.

2.1 Provisioning Tasks

To provision an ASE card, enter the following command in global configuration mode:

```
card ase slot
```

Commit the transaction.

2.2 Configuration Examples

The following example shows how to configure an ASE card in slot 4:

```
[local]Redback(config)#card ase 4
[local]Redback(config-card)#
```

3 Security Service Configuration

Security Service configuration consists of configuring ASP pools, configuring ASP groups, and associating a context with an ASP group. You can define ASP pools and groups at any time; however, and you can add an ASP to an ASP pool without an ASE card installed in the chassis. For information on ASP pools and ASP groups, see Reference [1].

3.1 ASP Pool Configuration

An ASP pool contains the following information:

- ASPs on ASE cards configured on the SmartEdge router that are assigned to this pool
- Specific security services provided by the ASPs in this pool

Note: Ensure that ASE and ASE2 card ASPs are not configured in the same pool.

3.1.1 Configuration Tasks

1. Configure the ASP pool in global configuration mode:

   ```
   (config)#asp pool pool-name service service-name
   ```

2. Add an ASP to the pool in ASP pool configuration mode:

   ```
   (cfg-asp-pool-mode)#asp slot-id/asp-id
   ```

3. Optional. Specify the maximum number of subscribers admitted for all ASPs associated with the pool.

   ```
   (cfg-asp-pool-mode)#maximum subscribers max-subscribers
   ```

4. Optional. Specify the maximum number of tunnels admitted for each ASP associated with the pool.

   ```
   (cfg-asp-pool-mode)#maximum tunnels ipsec max-tunnels
   ```

5. Commit the transaction.

3.1.2 Configuration Examples

The following example shows how to configure the `p1` ASP pool and specify six ASPs on four ASE cards to associate with the ASP pool:

Note: The service name for Security Service is `security`.

```
[local]Redback(config)#asp pool p1 service security
[local]Redback(cfg-asp-pool-mode)#asp 1/1
[local]Redback(cfg-asp-pool-mode)#asp 1/2
[local]Redback(cfg-asp-pool-mode)#asp 3/1
[local]Redback(cfg-asp-pool-mode)#asp 3/2
[local]Redback(cfg-asp-pool-mode)#asp 4/1
[local]Redback(cfg-asp-pool-mode)#asp 5/1
[local]Redback(cfg-asp-pool-mode)#maximum subscribers 16384
[local]Redback(cfg-asp-pool-mode)#maximum
tunnels ipsec 2048
```

3.2 ASP Group Configuration

An ASP group contains the following information:

- A reference to an ASP pool that provides the ASPs for the group.
- Number of ASPs requested from the ASP pool.
- Priority of the ASP group, which determines:

  a The distribution of ASPs to groups when the number of available ASPs is fewer than the total requested.

  b The ASP group that is allocated a newly operational ASP. The lower the number, the higher the priority.

3.2.1 Configuration Tasks

To configure an ASP group, enter the following commands:

1. Configure the ASP group in global configuration mode:

   ```
   (config)#asp group group-name
   ```

2. Associate the group with an existing ASP pool in ASP group configuration mode:

   ```
   (cfg-asp-group-mode)#pool pool-name
   ```

3. Specify the number of ASPs requested from the ASP pool in ASP group configuration mode:

   ```
   (cfg-asp-group-mode)#asp-count number
   ```

4. Specify the priority for the ASP group in ASP group configuration mode:

   ```
   (cfg-asp-group-mode)#priority number
   ```

5. Commit the transaction.

3.2.2 Configuration Examples

The following example shows how to configure the `g1` ASP group, associate the group with the `p1` ASP pool, specify that two ASPs must be associated with the ASP group, and set the priority to 100 for the ASP group:

```
[local]Redback(config)#asp group g1
[local]Redback(cfg-asp-group-mode)#pool p1
[local]Redback(cfg-asp-group-mode)#asp-count 2
[local]Redback(cfg-asp-group-mode)#priority 100
```

3.3 Enabling a Context to Provide an ASE Based Service

You enable a context to provide an ASE based security service, associate it with an ASP group, and identify the service. Associating the context with an ASP group directs traffic belonging to the context to the ASPs in the ASP group for processing.

In the current release, the only available ASE based service is `security` (Security Services). A context enabled to provide ASE based Security Services is called a security-enabled context.

3.3.1 Configuration Tasks

To configure a context to provide ASE based service, enter the following commands:

1. Configure the context in global configuration mode:

   ```
   (config)#context ctx-name
   ```

2. Associate the context with an existing ASP group and service in context configuration mode. You can associate all or some of the contexts to the same ASP group, or associate each context to a different ASP group.

   ```
   (config-ctx)#asp-group group-name service service-name
   ```

3. Commit the transaction.

3.3.2 Configuration Examples

The following example shows how to associate the `g1` ASP group with the `security` ASE based service within the `c3` context:

```
[local]Redback#context c3
[c3]Redback#config
[c3]Redback(config)#context C3
[c3]Redback(config-ctx)#asp-group g1 service security
```

4 Displaying ASP Pool and Group Information

Show commands display a variety of information for ASP pools and groups and for security-enabled contexts, as shown in Table 1.

Table 1 Show Commands

To display the following information…	**Enter this command…**
Summary information for all ASPs on all ASE cards installed in the SmartEdge router	`show asp`
Detailed information for a specific ASP.	`show asp` *`slot-id/asp-id`*
Summary ASP pool for all ASP pools.	`show asp pool`
Detailed information for all ASP pools.	`show asp pool detail`
Detailed information for a specific ASP pool.	`show asp pool` *`pool-name`*
Summary information for all ASP groups.	`show asp group`
Detailed information for all ASP groups.	`show asp group detail`
Detailed information for a specific ASP groups.	`show asp group` *`group-name`*

For more information about **`show`** commands see Reference [2].

5 Configuring Log Server Settings for Security Service

Reporting for advanced services is based on log messages. Log messages can be sent to the console or a log forwarding server and integrated with third-party reporting solutions or used by proprietary reporting solutions to generate deployment-specific reports. Log messages from all ASPs in all ASE cards installed in the SmartEdge router are sent using the specified ASP source to the specified log server. Each log message contains the system host name which must be set to a valid value; see the **`system`** command in Reference [4].

You must configure the source IP on the SmartEdge router for log messages that are forwarded to an external log server, such as the NetOp™ EMS Log Mediation server, and the IP address of the external log server. These settings are configurable default settings for the Security Service. No configuration is needed to control the generation of IKE or IPsec log messages from the IPsec VPN application. Additional configuration is required for the generation of P2P statistics; see Reference [3].

5.1 Configuration Tasks

To send log messages to a log forwarding server, perform the following steps:

1. Configure the default settings for the Security Service in global configuration mode.

   ```
   (config)#asp security default
   ```

2. Configure the IP address of the log forwarding server, and the optional transport protocol and forwarding port in ASP security default configuration mode.

   ```
   (config-asp-security-default)#log server server-ip
   transport transport-protocol port port
   ```

   The log server should be reachable through local context.

3. Configure the IP address of the log source and the context through which it is reachable:

   ```
   (config-asp-security-default)#log source source-ip
   context context
   ```

   The ***`source-ip`*** must be the IP address of a loopback interface in context local.

4. Commit the transaction.

5.2 Configuration Example

The following example configures logging to an external server:

```
[local]Redback(config)#asp security default
(config-asp-security-default)#log server 10.172.55.55
  transport udp port 514
(config-asp-security-default)#log source 10.192.22.24
  context c3
```

Glossary

ASE
Advanced Services Engine

ASE2
Advanced Services Engine 2

ASPs
Advanced Service Processors

CLI
Command Line Interface

DPI
Deep Packet Inspection

IPsec
Internet Protocol Security

UDP
User Datagram Protocol

VPN
Virtual Private Network

Reference List

[1] *Advanced Services Infrastructure Overview*, 1/221 02-CRA 119 1170/1-V1

[2] *Security Service Command Reference*, 1/190 80-CRA 119 1170/1-V1

[3] *Application Traffic Management Configuration and Operation*, 2/1543-CRA 119 1170/1-V1

[4] *Command List*, 1/190 77-CRA 119 1170/1-V1