ERICSSON

Traffic Redirection Configuration

OPERATION DIRECTIONS

6/1543-AXB 250 10/4-V3 Uen AY

Contents

1 Introduction

This document describes configuration of the automatic traffic redirection feature in the Service Aware Charging and Control (SACC) solution in the EPG for GSM, WCDMA, LTE systems, and trusted non-3GPP networks, such as CDMA2000.

1.1 Scope

This document covers the following issues:

— Detailed instructions for configuring header-based redirection and Uniform Resource Identifier (URI)-based redirection.

— Detailed instructions for configuring always-redirection, service denied redirection, one time redirection, final unit redirection, and initial redirection.

— Detailed instructions for configuring redirection constraints.

For an overview of traffic redirection, refer to Traffic Redirection.

1.2 Target Groups

This document is intended for personnel performing configuration of the EPG.

2 Activate Licensed Features

Optional licensed features in the EPG are turned off by default. To employ these features in the EPG, licenses must be purchased from Ericsson. For information on how to purchase licenses and enable licensed features, refer to Software License Management or contact your local Ericsson support.

To enable traffic redirection, activate the automatic redirection license.

3 Configure Traffic Redirection Methods

This section describes how to enable header-based redirection for certain header rules and URI-based redirection for certain HTTP-WSP rules.

3.1 Enable Header-Based Redirection

To enable header-based redirection for a header rule, include the following statement:

```
Ericsson(config)# epg pgw service-identification header-rule
<rule-name> term <term-id> then
   redirect-unauthorized
```

Header-based redirection can only be configured for header rules, that are configured to match protocol TCP or UDP. The statement is applicable for enabling redirection of all redirection types.

3.2 Enable URI-Based Redirection

To enable URI-based redirection for an HTTP-WSP rule, include the following statement:

```
Ericsson(config)# epg pgw service-identification http-wsp-rule
<rule-name> term <term-id> then
   redirect-unauthorized
```

The statement is applicable for enabling redirection of all redirection types.

The EPG applies redirection to HTTP responses or to both HTTP and WSP requests, depending on the classification of the HTTP-WSP rule. For more information, refer to PISC Configuration.

To enable URI-based redirection for default HTTP traffic with masquerading detection enabled, include the following statement:

```
Ericsson(config)# epg pgw service-set <service-set-name> serv
ice-identification enable-masquerading-detection
   http-enable-redirect
```

3.3 Enable HTTP Responses

To enable HTTP responses, follow the same steps to enable URI-based redirection, see Section 3.2 on page 2.

4 Configure Traffic Redirection Types

This section describes how to enable always-redirection, service denied redirection, one time redirection, final unit redirection, and initial redirection.

4.1 Enable Always-Redirection

This section describes how to enable always-redirection.

4.1.1 Enable Header-Based Always-Redirection

To enable header-based always-redirection, do the following:

1. Activate the automatic redirection license; see Section 2 on page 1.
2. Enable header-based redirection; see Section 3.1 on page 2.
3. Configure a header redirect set for always-redirected services; see Section 5.1.1 on page 6.
4. Configure a mapping of applicable Access Control Rules (ACRs) and the header redirect set, or configure the header redirect set as default; see Section 5.1.3 on page 7 or Section 5.1.4 on page 7.
5. Configure always-redirection condition for applicable ACRs, and optionally a mapping to a redirect reason; see Section 4.1.3 on page 3.

4.1.2 Enable URI-Based Always-Redirection

To enable URI-based always-redirection, do the following:

1. Activate the automatic redirection license; see Section 2 on page 1.
2. Enable URI-based redirection; see Section 3.2 on page 2.
3. Configure a URI redirect set for always-redirected services; see Section 5.2.1 on page 8.
4. Configure a mapping of applicable ACRs and the URI redirect set, or configure the URI redirect set as default; see Section 5.2.4 on page 8 or Section 5.2.5 on page 9.
5. Configure always-redirection condition for applicable ACRs, and optionally a mapping to a redirect reason; see Section 4.1.3 on page 3.

4.1.3 Configure Always-Redirection Condition for ACRs for a Rule Space

To configure always-redirection condition for an ACR or a consecutive range of ACRs separated by -, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-na
me> always-redirect
   access-control-rule (<acr-id> | <acr-id>-<acr-id>)
```

To configure the optional mapping between an ACR or a consecutive range of ACRs separated by -, and an always-redirect reason, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> always-re
direct access-control-rule (<acr-id> | <acr-id>-<acr-id>)
   reason <redirect-reason>
```

The redirect reason `default` is used if no specific redirect reason is configured for an always-redirected ACR. For a description of available redirect reasons, refer to Traffic Redirection.

4.2 Enable Service Denied Redirection

This section describes how to enable service denied redirection.

4.2.1 Enable Header-Based Service Denied Redirection

To enable header-based service denied redirection, do the following:

1. Activate the automatic redirection license; see Section 2 on page 1.
2. Enable header-based redirection; see Section 3.1 on page 2.
3. Configure a header redirect set for unauthorized services; see Section 5.1.2 on page 7.
4. Configure a mapping of applicable ACRs and the header redirect set, or configure the header redirect set as default; see Section 5.1.3 on page 7 or Section 5.1.4 on page 7.

4.2.2 Enable URI-Based Service Denied Redirection

To enable URI-based service denied redirection, do the following:

1. Activate the automatic redirection license; see Section 2 on page 1.
2. Enable URI-based redirection; see Section 3.2 on page 2.
3. Configure a URI redirect set for unauthorized services; see Section 5.2.2 on page 8.
4. Configure a mapping of applicable ACRs and the URI redirect set, or configure the URI redirect set as default; see Section 5.2.4 on page 8 or Section 5.2.5 on page 9.

4.3 Enable Service Denied HTTP Responses

To enable service denied HTTP responses, do the following:

1. Activate the automatic redirection license; see Section 2 on page 1.
2. Enable URI-based redirection; see Section 3.2 on page 2.
3. Configure an HTTP response profile; see Section 6.1 on page 9.
4. Configure an ACR mapping between the HTTP response profile and a blocking reason; see Section 6.2 on page 9.

   Note: For service denied HTTP responses, the ACRs must be configured as always denied ACRs.

4.4 Enable One Time Redirection

This section describes how to enable Gx interface one time redirection and Gy interface one time redirection.

4.4.1 Enable Gx Interface One Time Redirection

To enable URI-based one time redirection, do the following:

1. Activate the automatic redirection license; see Section 2 on page 1.
2. Enable URI-based redirection; see Section 3.2 on page 2.
3. Configure a URI redirect set for authorized services; see Section 5.2.3 on page 8.
4. Configure a mapping of applicable ACRs and the URI redirect set, or configure the URI redirect set as default; see Section 5.2.4 on page 8 or Section 5.2.5 on page 9.
5. Optionally, configure redirection constraints for one time redirection; see Section 7 on page 10.

4.4.2 Enable Gy Interface One Time Redirection

To enable URI-based one time redirection, do the following:

1. Activate the automatic redirection license; see Section 2 on page 1.
2. Enable URI-based redirection; see Section 3.2 on page 2.
3. Optionally, configure redirection constraints for one time redirection; see Section 7 on page 10.

4.5 Enable Final Unit Redirection

To enable URI-based final unit redirection, do the following:

1. Activate the automatic redirection license; see Section 2 on page 1.
2. Enable URI-based redirection; see Section 3.2 on page 2.
3. Optionally, configure redirection constraints for final unit redirection; see Section 7 on page 10.

4.6 Enable Initial Redirection

To enable URI-based initial redirection, do the following:

1. Activate the automatic redirection license; see Section 2 on page 1.
2. Enable URI-based redirection; see Section 3.2 on page 2.
3. Optionally, configure redirection constraints for initial redirection; see Section 7 on page 10.

5 Configure Traffic Redirection Destinations

A redirect set contains one or more redirect rules. Each rule specifies what redirect destination to be used for a specific redirect reason. If no redirect set is configured, no redirection is performed. This section describes how to configure redirect sets with redirect rules and how to associate redirect sets with ACRs.

5.1 Configure a Header Redirect Set

This section describes how to configure redirect rules for a header redirect set, and how to associate a header redirect set with ACRs.

5.1.1 Configure a Header Redirect Rule for Always-Redirected Services

To configure a header redirect rule for always-redirected services, specifying a destination for a redirect reason, include the following statement:

```
Ericsson(config)# epg pgw service-identification header-redirec
t-set <header-redirect-set-name> always <redirect-reason>
   destination-ipv4-address <destination-ipv4-address>
   destination-ipv6-address <destination-ipv6-address>
   destination-port <destination-port>
```

A destination can be configured for redirect reason `default`, to be used if no specific destination is configured for the actual reason. For a description of available redirect reasons, refer to Traffic Redirection. A destination address, a destination port, or both must be configured. At redirection, the EPG only replaces the specified fields in the packet headers. For example, if no destination port is configured in the redirect set, the original port is not replaced.

5.1.2 Configure a Header Redirect Rule for Unauthorized Services

To configure a header redirect rule for unauthorized services, specifying a destination for a redirect reason, include the following statement:

```
Ericsson(config)# epg pgw service-identification header-redirect-s
et <header-redirect-set-name> unauthorized <redirect-reason>
   destination-ipv4-address <destination-ipv4-address>
   destination-ipv6-address <destination-ipv6-address>
   destination-port <destination-port>
```

A destination can be configured for redirect reason `default`, to be used if no specific destination is configured for the actual reason. For a description of available redirect reasons, refer to Traffic Redirection. A destination address, a destination port, or both must be configured. At redirection, the EPG only replaces the specified fields in the packet headers. For example, if no destination port is configured in the redirect set, the original port is not replaced.

5.1.3 Configure a Mapping of ACRs and Header Redirect Sets for a Rule Space

A mapping between ACRs and header redirect sets is optional and determines which set of redirect rules to employ for specific services. If no mapping is configured for an ACR, the default header redirect set is used; see Section 5.1.4 on page 7.

To configure a mapping between a header redirect set and an ACR or a consecutive range of ACRs separated by -, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> redi
rect-map <header-redirect-set-name>
   access-control-rule (<acr-id> | <acr-id>-<acr-id>)
```

5.1.4 Configure a Default Header Redirect Set for a Rule Space

A default header redirect set is optional and is used if no mapping is configured between an ACR and a header redirect set; see Section 5.1.3 on page 7.

To configure a default header redirect set, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name>
   default-header-redirect-set <header-redirect-set-name>
```

5.2 Configure a URI Redirect Set

This section describes how to configure redirect rules for an URI redirect set, and how to associate an URI redirect set with ACRs.

5.2.1 Configure a URI Redirect Rule for Always-Redirected Services

To configure a URI redirect rule for always-redirected services, specifying a destination for a redirect reason, include the following statement:

```
Ericsson(config)# epg pgw service-identification uri-redirect-set
<uri-redirect-set-name> always <redirect-reason>
   uri <destination-uri>
```

A destination can be configured for redirect reason `default`, to be used if no specific destination is configured for the actual reason. For a description of available redirect reasons, refer to Traffic Redirection. URI formatting codes can be appended to the URI configured in a redirect rule. For a description of available formatting codes, refer to Traffic Redirection.

5.2.2 Configure a URI Redirect Rule for Unauthorized Services

To configure a URI redirect rule for unauthorized services, specifying a destination for a redirect reason, include the following statement:

```
Ericsson(config)# epg pgw service-identification uri-redirect-set
<uri-redirect-set-name> unauthorized <redirect-reason>
   uri <destination-uri>
```

A destination can be configured for redirect reason `default`, to be used if no specific destination is configured for the actual reason. For a description of available redirect reasons, refer to Traffic Redirection. URI formatting codes can be appended to the URI configured in a redirect rule. For a description of available formatting codes, refer to Traffic Redirection.

5.2.3 Configure a URI Redirect Rule for Authorized Services

To configure a URI redirect rule for authorized services, specifying a destination for a redirect reason, include the following statement:

```
Ericsson(config)# epg pgw service-identification uri-redirect-set
<uri-redirect-set-name> authorized <redirect-reason>
   uri <destination-uri>
```

For a description of available redirect reasons, refer to Traffic Redirection. URI formatting codes can be appended to the URI configured in a redirect rule. For a description of available formatting codes, refer to Traffic Redirection.

5.2.4 Configure a Mapping of ACRs and URI Redirect Sets for a Rule Space

A mapping between ACRs and URI redirect sets is optional and determines which set of redirect rules to employ for specific services. If no mapping is configured for an ACR, the default URI redirect set is used; see Section 5.2.5 on page 9.

To configure a mapping between a URI redirect set and an ACR or a consecutive range of ACRs separated by -, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> redi
rect-map <uri-redirect-set-name>
   access-control-rule (<acr-id> | <acr-id>-<acr-id>)
```

5.2.5 Configure a Default URI Redirect Set for a Rule Space

A default URI redirect set is optional and is used if no mapping is configured between an ACR and a URI redirect set; see Section 5.2.4 on page 8.

To configure a default URI redirect set, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name>
   default-uri-redirect-set <uri-redirect-set-name>
```

6 Configure Traffic Redirection of HTTP Responses

6.1 Configure HTTP Response

To configure an HTTP response, include the following statement:

```
Ericsson(config)# epg pgw service-identification http-re
sponses response <response-name>
   status-code <response-code>
   message-body <response-content>
```

Note: The following HTML formatting characters are not supported in the message body: `<,>,%," "`.

6.2 Configure Mapping of ACRs and HTTP Response Rules

To configure a mapping of ACRs and an HTTP response rule, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> acces
s-control-rule <acr-id> http-response-rule
   response <response-name>
   reason <blocking-reason>
```

7 Configure Traffic Redirection Constraints

Traffic redirection constraints using user agent filtering is based on a set of textual match rules, against which the user agent of a redirectable packet is compared. The redirection constraints also contain a default policy for user agents that do not match the rules. With a default policy not to redirect traffic, a set of rules can be defined to match user agents allowed for redirection. Redirectable traffic of authorized services is let through instead of redirected if the redirection constraints do not allow redirection. Redirectable traffic of unauthorized services is dropped instead of redirected if redirection constraints do not allow redirection.

7.1 Configure a Rule for User Agents

For information on how to configure a text rule and a text rule set, refer to PISC Configuration.

7.1.1 Configure a Text Rule with a Term to Match User Agents

To configure a text rule with a term to match user agents, include the following statement:

```
Ericsson(config)# epg pgw service-identification text-r
ule <rule-name> term <term-id>
   starts-with <string>
```

7.1.2 Associate a Text Rule with a Text Rule Set to Match User Agents

To configure a text rule set of text rules, include the following statement:

```
Ericsson(config)# epg pgw service-identification text-rule-set
<rule-set-name> rule <rule-id>
   name <rule-name>
```

7.2 Configure a Set of Allowed User Agents

To configure a text rule set to match user agents allowed for redirection, include the following statement:

```
Ericsson(config)# epg pgw service-identification redirect-constraints user-a
   allowed <rule-set-name>
```

7.3 Configure the Default Policy

To configure the default policy to not allow redirection for user agents that do not match the configured text rules, include the following statement:

```
Ericsson(config)# epg pgw service-identification redirect-constraints user-a
   default not-allowed
```

7.4 Enable Redirection Constraints for a Rule Space

This section describes how to enable redirection constraints for a rule space and a redirection type.

7.4.1 Enable Redirection Constraints for One Time Redirection

To enable redirection constraints for a rule space and one time redirection, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-nam
e> redirect-constraints
   one-time
```

7.4.2 Enable Redirection Constraints for Final Unit Redirection

To enable redirection constraints for a rule space and final unit redirection, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-nam
e> redirect-constraints
   final
```

7.4.3 Enable Redirection Constraints for Initial Redirection

To enable redirection constraints for a rule space and initial redirection, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-nam
e> redirect-constraints
```

```
initial
```