Configuring HTTP Redirect

SYSTEM ADMINISTRATOR GUIDE

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.

Contents

1 Overview

This document provides an overview of the HTTP redirect features on the SmartEdge® router and describes the tasks used to configure, monitor, and administer HTTP redirect. This document also provides a configuration example of HTTP redirect.

HTTP redirect enables service providers to interrupt subscriber HTTP sessions and to redirect them to a preconfigured URL. By default, a message displays to the subscriber for a period of time while the subscriber HTTP session is redirected to a preconfigured URL. The default message reads "Please wait while you are redirected . . ..." and the default timeout period is one second. You have the option of configuring a customized HTTP redirect message and timeout period. You also have the option of providing the subscriber's identity attributes along with the URL and encrypt this data. You also have the option of modifying your HTTP redirect configuration to allow for per-class URLs.

Applications of the HTTP redirect feature include the ability to require customer registration, to direct customers to web sites for downloading virus protection software, and to advertise new services or software updates.

Note: In the following descriptions, the term, controller card, applies to the Cross-Connect Route Processor (XCRP4) Controller card, unless otherwise noted.

The SmartEdge router provides a lightweight HTTP server on its controller card. When a subscriber initiates an HTTP session, authentication triggers an HTTP redirect when two conditions are in place: an HTTP redirect profile containing a new URL is attached to the subscriber record, and a forward policy that redirects HTTP traffic to the HTTP server on the controller card is attached to the subscriber circuit. HTTP packets must be permitted to pass through to the external HTTP server that hosts the redirect URL. The subscriber session opens to the web page indicated by the redirect URL. The forward policy that performs the redirection is removed through the subscriber reauthorization mechanism.

1.1 IPv6 HTTP Redirect Policies

- With IPv6 forwarding, HTTP redirect is limited to local URLs.
- VSA 165 HTTP URL can be configured as type `v4` or `v6`.
- VSA 107 HTTP profile is unchanged with IPv6 policies.
- An HTTP profile itself can be configured with IPv4 and IPv6 URLs.
- The VSA 165 HTTP URL has higher precedence than an HTTP profile.

- If an HTTP server is configured with both URL types, it redirects IPv4 traffic to v4 URLs and IPv6 traffic to v6 URLs.
- If an HTTP server is only configured with an IPv4 URL, it redirects both IPv4 and IPv6 traffic to the IPv4 URL.
- If an HTTP server is only configured with an IPv6 URL, it redirects both types of traffic to the IPv6 URL.

2 Configuration and Operations Tasks

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

To configure, monitor, and troubleshoot HTTP redirect features, perform the tasks described in the following sections:

2.1 Configure Subscriber Authentication and Reauthorization

To configure subscriber authentication and reauthorization, see *Configure Subscriber Authentication* and *Configure Dynamic Subscriber Reauthorization*.

2.2 Configure an IP ACL and Apply It to Subscribers

To redirect subscriber traffic to the new web page to which subscriber circuits are to be redirected, configure an IP access control list (ACL) that permits access to that web page and applies it to the subscriber circuits (their records or profiles) that are to be redirected. To configure and apply an IP ACL, see *Configuring ACLs*.

2.3 Configure the HTTP Server on the Active Controller Card

To configure the HTTP server on the active controller card, perform the following tasks:

1. Enable the HTTP server on the controller card and access HTTP redirect server configuration mode using the *http-redirect server* command in global configuration mode.

2. Optional. Select the port on which HTTP server listens with the *port (http)* command in HTTP redirect server configuration mode.

2.4 Configure and Attach an HTTP Redirect Profile to Subscribers

To configure and attach an HTTP redirect profile to subscribers, perform the following tasks in HTTP redirect profile configuration mode, unless otherwise noted.:

1. Configure an HTTP redirect profile and access HTTP redirect profile configuration mode using the *http-redirect profile* command in context configuration mode.

2. Optional. Configure the http-redirect message to display to the subscriber before the http-subscriber session is redirected with the *message* command.

3. Optional. Sets the maximum time the SmartEdge router displays the customized HTTP redirect message to the subscriber before the subscriber HTTP session is redirected to the preconfigured URL with the *timeout (HTTP redirect)* command.

4. Configure the URL to which subscriber sessions are to be redirected using the *url* command.

5. Configure the IPv6 URL (to which subscriber sessions are to be redirected) using the *ipv6 url* command.

6. Attach the HTTP redirect profile to a subscriber record, a named subscriber profile, or the default subscriber profile using the *http-redirect profile* in subscriber configuration mode.

Caution!

Risk of redirect loop. Redirect can recur until an IP ACL that permits access to the new web page is applied to the subscriber record or profile. To reduce the risk, before modifying an existing URL, ensure that the subscriber record includes an IP ACL that permits access to the new URL.

The SmartEdge OS applies an HTTP profile in the following order of precedence:

1. Uses the vendor-specific attribute (VSA) 107 provided by Ericsson AB, HTTP-Redirect-Profile-Name, in the subscriber record returned by the RADIUS server in Access-Accept packets for the subscriber.

2. Limits using one URL VSA per subscriber (either IPv6 or ipv4) and forces using an HTTP profile when configuring both an IPv4 and IPv6 URL.

3. If the RADIUS server does not return an HTTP profile name, it uses the HTTP profile attached to the named subscriber configured in the context.

4. If the named subscriber does not have an HTTP profile attached to it, then it uses the HTTP profile attached to the named subscriber profile configured in the context.

5. If the subscriber profile does not have an HTTP profile attached to it, then it uses the HTTP profile attached to the default subscriber profile configured in the context.

2.5 Configure a Policy ACL That Classifies HTTP Packets

To configure a policy access control list (ACL) that classifies HTTP packets for the forward policy that redirects HTTP packets, perform the following tasks as appropriate:

1. Create or select the IPv4 policy ACL and enter access control list configuration mode using the *policy access-list* command in context configuration mode.

2. Create or select the IPv6 policy ACL and enter access control list configuration mode using the *ipv6 policy access-list* command in context configuration mode.

3. Assign HTTP packets that are destined to the web server hosting the URL to a separate class using the *permit* command in access control list configuration mode.

   Use the following construct: **`permit tcp any host`** ***`ip-addr`*** **`eq www class`** ***`class-name`*** where the ***`ip-addr`*** argument is the IP address of the web server hosting the URL that you configured (using the **`url`** or **`ipv6-url`** command) in Section 2.4 on page 3.

4. Assign all other HTTP packets to a different class using the *permit* command in access control list configuration mode.

   Use the following construct: **`permit tcp any any eq www class`** ***`class-name`*** where the ***`class-name`*** argument is distinct from the one you configured in Section 2.4 on page 3.

2.6 Configure and Attach a Forward Policy to Redirect HTTP Packets

To configure a forward policy to redirect HTTP packets and attach it to a circuit or subscriber, perform the following tasks.

1. Create or select the forward policy and access forward policy configuration mode using the*forward policy* command in global configuration mode.

   For more information about forward policies, see *Configuring Forward Policies*.

2. Apply the policy IPv4 ACL that you configured in Section 2.5 on page 5 to the forward policy and access policy ACL configuration mode using the *ip access-group* command in forward policy configuration mode.

3. Apply the policy IPv6 ACL that you configured in Section 2.5 on page 5 to the forward policy and access policy ACL configuration mode using the *ipv6 access-group* command in forward policy configuration mode.

4. Specify all HTTP packets and access policy ACL class configuration mode using the *class* command in policy ACL configuration mode.

   Use the ***`class-name`*** argument that you specified in step 3 in Section 2.5 on page 5.

5. Redirect HTTP packets to the HTTP server on the controller card using the *redirect destination local* command in policy ACL class configuration mode.

6. Attach the forward policy to a circuit, a subscriber record, named subscriber profile, or default subscriber profile using the *forward policy in* command.

   Enter this command in ATM OC, ATM PVC, dot1q PVC, Frame Relay PVC, port, or subscriber configuration mode.

   For more information about forward policies, see *Configuring Forward Policies*.

2.7 Operations Tasks

To monitor and troubleshoot the HTTP redirect features, perform the appropriate HTTP redirect operations tasks described in Table 1. Enter the **`debug`** command in exec mode; enter the **`show`** commands in any mode.

Table 1 HTTP Redirect Operations Tasks

Step	Task	Command
1.	Enable the generation of debug messages for the HTTP redirect events and error messages. You can also filter debug messages by policies, sessions, and subscribers.	*debug hr*
2.	Display the current HTTP redirect configuration.	*show configuration hr*
3.	Display HTTP redirect circuit information.	*show http-redirect circuit*

3 Configuration Examples

The following example provides a simple IPv4 HTTP redirect configuration:

```
!First enable the HTTP redirect server on the controller card:
[local]Redback(config)#http-redirect server
[local]Redback(config-hr-server)#port 80 8080
[local]Redback(config-hr-server)#exit

!Configure the HTTP redirect profile, customized http-redirect message, timeout and url:
[local]Redback(config)#context local
[local]Redback(config-ctx)#http-redirect profile Redirect
[local]Redback(config-hr-profile)#message “Please wait while you are redirected to the
customer portal server. Thank you.”
[local]Redback(config-hr-profile)#timeout 30
[local]Redback(config-hr-profile)#url http://www.Redirect.com
[local]Redback(config-hr-profile)#exit

!Attach the HTTP redirect profile to the default subscriber profile:
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#http-redirect profile Redirect
[local]Redback(config-sub)#exit

!Create a policy ACL:
[local]Redback(config-ctx)#policy access-list http-packets
!Create class abc for HTTP packets that are destined to the web server with the new URL:
[local]Redback(config-access-list)#permit tcp any host 10.1.1.1 eq www class abc

!Create class xyz for all other HTTP packets to be redirected using the forward policy:
[local]Redback(config-access-list)#permit tcp any any eq www class xyz
[local]Redback(config-ctx)#exit

!Create the forward policy:
[local]Redback(config)#forward policy www-redirect

!Apply the policy ACL that classifies HTTP packets:
[local]Redback(config-policy-frwd)#ip access-group http-packets local
```

```
!Redirect all HTTP packets except those destined to the web server (class xyz):

!to the HTTP server on the controller card:
[local]Redback(config-policy-group)#class xyz
[local]Redback(config-policy-group-class)#redirect destination local
[local]Redback(config-policy-group-class)#exit

!Packets that are destined to the web server (class abc) use normal routing (no action).
[local]Redback(config-policy-group)#class abc
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-frwd)#exit

!Attach the forward policy to incoming packets on ATM PVC 3 5:
[local]Redback(config)#port atm 4/1
[local]Redback(config-atm)#no shutdown
[local]Redback(config-atm-oc)#atm pvc 3 5 profile atm-pro encapsulation bridge1483
[local]Redback(config-atm-pvc)#forward policy www-redirect in

!Bind the appropriate subscriber record to the ATM PVC:
[local]Redback(config-atm-pvc)#bind subscriber joe@local
```

The following example provides a simple HTTP redirect configuration for both IPv4 and IPv6:

```
!First enable the HTTP redirect server on the controller card:

[local]Redback(config)#http-redirect server
[local]Redback(config-hr-server)#port 80 8080
[local]Redback(config-hr-server)#exit

!Configure the HTTP redirect profile, customized http-redirect message, encryption

[local]Redback(config)#context local
[local]Redback(config-ctx)#http-redirect profile Redirect
[local]Redback(config-hr-profile)#message
“Please wait while you are redirected to the customer portal server. Thank you.”
[local]Redback(config-hr-profile)#encrypt secret29$%*() delimiter :
[local]Redback(config-hr-profile)#timeout 30
[local]Redback(config-hr-profile)#url http://www.Redirect.com
[local]Redback(config-hr-profile)#ipv6 url http://ipv6.Redirect.com
[local]Redback(config-hr-profile)#exit
```

```
!Attach the HTTP redirect profile to the default subscriber profile:
[local]Redback(config-ctx)#subscriber default
[local]Redback(config-sub)#http-redirect profile Redirect
[local]Redback(config-sub)#Forward policy www-redirect in
!Note: Forward policy can be configured here (under "subscriber default") to be

!Create a policy ACL:

[local]Redback(config)#context local
[local]Redback(config-ctx)#policy access-list http-packets<<<< This is an ipv4 p
!Create class abc for HTTP packets that are destined to the web server with the
[local]Redback(config-access-list)#permit tcp any host 10.1.1.1 eq www class abc
[local]Redback(config-access-list)#ipv6 policy access-list http-packets
[local]Redback(config-ipv6-access-list)#permit ipv6 2001:a:b:1::/64 any class ab
[local]Redback(config-ipv6-access-list)#forward policy www-redirect
[local]Redback(config-policy-frwd)#ip access-group http-packets local
[local]Redback(config-policy-group)#ipv6 access-group http-packets local
[local]Redback(config-policy-group)#class abc
[local]Redback(config-policy-group-class)#redirect destination local
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-frwd)#exit

!Create class xyz for all other HTTP packets to be redirected using the forward

[local]Redback(config-access-list)#permit tcp any any eq www class xyz
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#exit
[local]Redback(config)#context local
[local]Redback(config-ctx)#policy access-list
[local]Redback(config-ctx)#policy access-list http-packets
[local]Redback(config-access-list)#permit tcp any any eq www class xyz
[local]Redback(config-access-list)#exit
[local]Redback(config-ctx)#exit

!Create the forward policy:

[local]Redback(config)#forward policy www-redirect

!Apply the policy ACL that classifies HTTP packets:

[local]Redback(config-policy-frwd)#ip access-group http-packets local

!Redirect all HTTP packets except those destined to the web server (class xyz):


!to the HTTP server on the controller card:

[local]Redback(config-policy-group)#class xyz
[local]Redback(config-policy-group-class)#redirect destination local
```

```
[local]Redback(config-policy-group-class)#exit

!Packets that are destined to the web server (class abc) use normal routing (no ac

[local]Redback(config-policy-group)#class abc
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-frwd)#exit

!Attach the forward policy to incoming packets on ATM PVC 3 5:

[local]Redback(config)#port atm 4/1
[local]Redback(config-atm)#no shutdown
[local]Redback(config-atm-oc)#atm pvc 3 5 profile atm-pro encapsulation bridge1483
[local]Redback(config-atm-pvc)#forward policy www-redirect in

!Bind the appropriate subscriber record to the ATM PVC:

[local]Redback(config-atm-pvc)#bind subscriber joe@local
```