Contents

Configuring HTTP redirect

About HTTP redirect

HTTP redirect is a method to redirect users' HTTP or HTTPS requests to a specific URL. It is used in the following features:

- Redirect URL assignment in 802.1X authentication, MAC authentication, Web authentication, and port security.
- EAD assistant URL redirection in 802.1X authentication.
- URL redirection services in portal.

HTTP redirect tasks at a glance

No configuration is required to redirect HTTP requests.

To redirect HTTPS requests, perform the following tasks:

1. Specifying the HTTPS redirect listening port number
2. (Optional.) Associating an SSL server policy with the HTTPS redirect service

Specifying the HTTPS redirect listening port number

About the HTTPS redirect listening port number

The device can redirect HTTPS requests only after you specify the TCP port number on which the HTTPS redirect service listens for HTTPS requests.

Restrictions and guidelines

To avoid service unavailability caused by port conflict, do not specify a TCP port number used by a well-known protocol or used by any other TCP-based service. To display TCP port numbers that have been used by services, use the **display tcp** command. For more information about this command, see IP performance optimization commands in *Layer 3—IP Services Command Reference*.

If you perform this task multiple times, the most recent configuration takes effect.

Procedure

1. Enter system view.

   system-view
2. Specify the HTTPS redirect listening port number.

   http-redirect https-port *port-number*

   By default, the HTTPS redirect listening port number is 6654.

Associating an SSL server policy with the HTTPS redirect service

About associating an SSL server policy with the HTTPS redirect service

To improve the security of HTTPS redirect, you can associate an SSL server policy with the HTTPS redirect service. For more information about the SSL server policy configuration, see SSL in *Security Configuration Guide*.

Restrictions and guidelines

HTTPS redirect is unavailable if the associated SSL server policy does not exist. You can first associate a nonexistent SSL server policy with the HTTPS redirect service and then configure the SSL server policy.

If you change the SSL server policy associated with the HTTPS redirect service, the new policy takes effect immediately.

If you perform this task multiple times, the most recent configuration takes effect.

Procedure

1. Enter system view.

   `system-view`

2. Associate an SSL server policy with the HTTPS redirect service.

   `http-redirect ssl-server-policy` *`policy-name`*

   By default, no SSL server policy is associated with the HTTPS redirect service. The HTTPS redirect service uses the self-assigned certificate and the default SSL parameters.