Table of Contents

CAPTCHA Page Creation

The CAPTCHA page is intended to block requests from botnets.

The CAPTCHA page should be placed behind the DPI (support for hosting CAPTCHA on external resources, e.g., Cloudflare, is planned) and service 10 with a protection profile should also be applied to it. At a minimum, the profile should include the parameters ddos_check_server and ddos_security_key. For simplicity, the same profile used for the protected site can be reused.

The CAPTCHA page should be lightweight to withstand a large number of attacking computers.

The parameter UrlRedir, containing the URL of the protected site the user was attempting to reach, is passed to the page.

After completing the CAPTCHA check, an internal redirect should be performed on the CAPTCHA page with an encrypted parameter signaling the DPI that the protection has been passed, after which the user can be redirected to the protected site using the UrlRedir parameter.

Successful CAPTCHA entry indicates that a human has accessed the site. Service 8 will be automatically applied to the user's IP, allowing them to access the protected site without repeating the CAPTCHA. It is advisable to periodically reset this service, as previously clean computers may become infected.

The rules for generating the security token and an example CAPTCHA page can be obtained from the support team.