

ABSTRACT

Embodiments of the present disclosure provide a method and apparatus for processing data. A specific embodiment of the method includes: receiving an access request to access a target domain name; converting the target domain name into a preset high defense domain name; querying an IP corresponding to the high defense domain name in a domain name system; and sending the access request according to the IP corresponding to the high defense domain name; where in a case that an EIP corresponding to the target domain name enables a black hole, the IP corresponding to the high defense domain name in the domain name system is a preset high defense IP, and in a case that the EIP corresponding to the target domain name closes the black hole, the IP corresponding to the high defense domain name in the domain name system is the EIP of the target domain name. In this embodiment, the whole process of scheduling a high defense IP from triggering a black hole to releasing the black hole and the switching of the high defense IP may be completed automatically without the user's participation. This solution guarantees the availability of services when being attacked, and guarantees the best experience of user services under normal circumstances.

Fig. 2