CLAIMS:

1. A traffic processing method performed by a protection device, comprising:

detecting incoming traffic flowing to a server to determine whether the server is attacked by a distributed denial of service (DDoS);

in response to determining that the server is attacked by the distributed denial of service (DDoS), determining whether a message format of a message in the incoming traffic is normal, and intercepting the message with an abnormal message format, wherein the incoming traffic is generated based on a quick user datagram protocol internet connection (QUIC) protocol; and

intercepting an abnormal message in a first message, wherein the first message is a message with a normal message format;

wherein the intercepting of the abnormal message in the first message comprises:

obtaining, for the first message, a message type of the first message; and

intercepting the abnormal message in the first message according to a protection policy corresponding to the message type of the first message;

wherein the intercepting of the abnormal message in the first message according to the protection policy corresponding to the message type of the first message comprises:

determining the message carrying a target session identifier from a non-initial message in the first message, wherein in the QUIC protocol, messages belonging to different sessions use different session identifiers, and a number of times that the target session identifier appears in a session within a first preset time reaches a first preset number of times; and

discarding the message carrying the target session identifier.

2. The traffic processing method according to claim 1, wherein in response to determining that the server is attacked by the distributed denial of service (DDoS), the determining of whether the message format of the message in the incoming traffic is normal, and the intercepting of the message with the abnormal message format comprises:

determining a second message with a message header that is a short header data packet in the incoming traffic in response to determining that the server is attacked by the distributed denial of service (DDoS);

determining that the message format of the second message is abnormal and discarding the

second message in response to a length of a user datagram protocol (UDP) load of the second message being less than a length corresponding to a first preset byte; and

determining that the message format of the second message is normal in response to the length of the UDP load of the second message being greater than or equal to the length corresponding to the first preset byte.

3. The traffic processing method according to claim 1, wherein in response to determining that the server is attacked by the distributed denial of service (DDoS), the determining of whether the message format of the message in the incoming traffic is normal, and the intercepting of the message with the abnormal message format comprises:

determining a third message with a message header that is a long header data packet in the incoming traffic in response to determining that the server is attacked by the distributed denial of service (DDoS); and

determining that the message format of the third message is abnormal and discarding the third message in response to a length of a user datagram protocol (UDP) load of the third message being less than a length corresponding to a second preset byte.

4. The traffic processing method according to claim 3, wherein in response to determining that the server is attacked by the distributed denial of service (DDoS), the determining of whether the message format of the message in the incoming traffic is normal, and the intercepting of the message with the abnormal message format further comprises:

determining whether the third message is an initial message in response to the length of the UDP load of the third message being greater than or equal to the length corresponding to the second preset byte, wherein the initial message is configured to request for establishing connection by a target client initiating the initial message; and

determining that the message format of the third message is abnormal and discarding the third message in response to the third message being the initial message and the length of the UDP load of the third message being less than a length corresponding to a third preset byte, wherein the second preset byte is less than the third preset byte.

5. The traffic processing method according to claim 4, wherein in response to determining

that the server is attacked by the distributed denial of service (DDoS), the determining of whether the message format of the message in the incoming traffic is normal, and the intercepting of the message with the abnormal message format further comprises:

determining that the message format of the third message is normal in response to the third message being not the initial message and the length of the UDP load of the third message being greater than or equal to the length corresponding to the second preset byte; and

determining that the message format of the third message is normal in response to determining that the third message is the initial message and the length of the UDP load of the third message is greater than or equal to the length corresponding to the third preset byte.

6. The traffic processing method according to claim 1, wherein the intercepting of the abnormal message in the first message according to the protection policy corresponding to the message type of the first message comprises:

for an initial message in the first message, sending, instead of the server, a response message to a target client corresponding to the initial message, wherein the initial message is configured to request for establishing connection by the target client, the response message carries a random character and is configured to instruct the target client to resend the initial message, and the initial message resent by an abnormal client does not carry the random character, and the initial message resent by a normal client carries the random character;

receiving the initial message resent by the target client and verifying whether the initial message resent by the target client carries the random character; and

in response to the initial message resent by the target client not carrying the random character, returning to the sending, instead of the server, the response message to the target client corresponding to the initial message to intercept an abnormal message in the message with the normal message format.

7. The traffic processing method according to claim 6, further comprising:

in response to the initial message resent by the target client carrying the random character, adding the target client to a trust list, and sending an interrupting connection message to the target client, wherein the interrupting connection message is configured to interrupt connection between the target client and the protection device, and the message generated by a client added to the trust

list is directly sent to the server.

8. The traffic processing method according to claim 1, wherein the determining of the message carrying the target session identifier from the non-initial message in the first message comprises:

obtaining five-tuple information corresponding to the non-initial message in the first message, wherein the five-tuple information comprises a source internet protocol (IP) address, a source port, a target IP address, a target port and a protocol type; and

determining the message carrying the target session identifier from the non-initial message in the first message according to the five-tuple information.

9. The traffic processing method according to claim 1, wherein the intercepting of the abnormal message in the first message according to the protection policy corresponding to the message type of the first message comprises:

determining the message carrying a target effective load from a non-initial message in the first message, wherein the target effective load is an effective load with a number of times that the effective load appears among all effective loads within a second preset time reaching a second preset number of times; and

discarding the message carrying the target effective load.

10. The traffic processing method according to claim 9, wherein first preset bytes of target effective loads are the same, last preset bytes of the target effective loads are the same, and the target effective load is the effective load with the number of times that the effective load appears among all effective loads within the second preset time reaching the second preset number of times.

11. The traffic processing method according to claim 1, wherein the detecting of the incoming traffic flowing to the server to determine whether the server is attacked by the distributed denial of service (DDoS) comprises:

detecting mirror traffic obtained by performing mirroring on the incoming traffic flowing to the server to count a real-time packet total of a port 443 of the server in real time, wherein the port 443 is a port used by the QUIC protocol;

determining that the server is attacked by the distributed denial of service (DDoS) in response to the real-time packet total being greater than an attack threshold; and

determining that the server is not attacked by the distributed denial of service (DDoS) in response to the real-time packet total being less than or equal to the attack threshold.

12. A traffic processing apparatus, comprising:

a detection module configured to detect incoming traffic flowing to a server to determine whether the server is attacked by a distributed denial of service (DDoS);

a first protection module configured to, in response to determining that the server is attacked by the distributed denial of service (DDoS), determine whether a message format of a message in the incoming traffic is normal, and intercept the message with an abnormal message format, wherein the incoming traffic is generated based on a quick user datagram protocol internet connection (QUIC) protocol; and

a second protection module configured to intercept an abnormal message in a first message, wherein the first message is a message with a normal message format;

wherein the second protection module comprises: a first obtaining sub-module configured to obtain, for the first message, a message type of the first message; and a first interception sub-module configured to intercept the abnormal message in the first message according to a protection policy corresponding to the message type of the first message; and

the second protection module further comprises: a tenth determining sub-module configured to determine the message carrying a target session identifier from a non-initial message in the first message, wherein in the QUIC protocol, messages belonging to different sessions use different session identifiers, and a number of times that the target session identifier appears in a session within a first preset time reaches a first preset number of times; and a second interception sub-module configured to discard the message carrying the target session identifier.

13. A computer-readable medium having a computer program stored thereon that, when executed by a processing device, implements the traffic processing method according to any of claims 1 to 11.

14. An electronic device, comprising:

a storage device having a computer program stored thereon; and

a processing device configured to execute the computer program in the storage device to implement the traffic processing method according to any of claims 1 to 11.