

device is shown in FIG. 7. The security device includes a processor, a non-volatile storage medium, an internal memory, and a network interface which are coupled via a system bus. The non-volatile storage medium of the security device stores an operating system and at least one computer executable instruction, which may be executed by the processor. The processor is configured to provide computation and control capabilities to support the entire operation of the security device. The internal memory of the security device provides a cached operating environment for the operating system and the computer executable instruction in the non-volatile storage medium. The network interface is configured to communicate with the server shown in FIG. 6 over a network connection. A person skilled in the art should understand that, the structure of the security device shown in FIG. 7 is only a part of the structure related to the solutions of the present application, which does not constitute limitation to the security device that the solutions of the present application apply to. A particular security device can include more or less components than those shown in the drawing, or can combine some components, or can have different component arrangement.

In one embodiment, a security device is provided, and when the processor of the security device executes the computer executable instructions in the memory, the processor of the security device specifically performs the following steps, including: detecting network/system state information and user behavior information in a network/system environment according to an own defense policy to generate security log information; uploading the generated security log information to a security log sharing platform, wherein the security log sharing platform is configured to classify and summarize the uploaded security log information, to generate a plurality of event types of intrusion event information, and to push the plurality of event types of intrusion event information according to a preset rule; receiving at least one of the event types of intrusion event information which is pushed by the security log sharing platform; and generating a joint defense policy by taking the received intrusion event information as clue information.

In one embodiment, the generating a joint defense policy by taking the received intrusion event information as clue information performed by the processor includes: associating the security log information generated by the security device itself with the received intrusion event information to generate joint security log information; and generating a joint defense policy according to the joint security log information, and implementing the joint defense policy to perform intrusion event detection and intrusion event defense.

Each of the above modules may be implemented in all or in part by software, hardware, and combinations thereof. The network interface may be an Ethernet card or a wireless network card. Each of the above modules may be embedded in or independent of the processor in the server and the security device in a form of hardware, or may be stored in the memory in the server and the security device in a form of software, which is easy to be called by the processor to perform the

CLAIMS

1. A method for network security joint defense, comprising:

obtaining security log information of a plurality of security devices, wherein the security log information includes intrusion event information violating an own defense policy of the security device obtained by the security device in a network/system environment;

classifying and summarizing the intrusion event information included in the security log information according to preset intrusion event types;

obtaining a corresponding relationship between each preset intrusion event type and a security device identification; and

pushing the intrusion event information which is summarized according to the intrusion event types to the security device directed to by the security device identification having a corresponding relationship, so that the security device adjusts its own defense policy according to the pushed intrusion event information.

2. The method according to claim 1, wherein after obtaining security log information of a plurality of security devices, the method further comprises:

converting log formats of the multiple obtained security log information into a preset log format, wherein the preset log format is a log format that is identifiable by the plurality of the security devices.

3. The method according to claim 1 or 2, wherein the security device comprises a fuzzy detection device and an attack detection device, the fuzzy detection device is configured to detect a fuzzy intrusion event, the attack detection device is configured to detect attack source information, and the detected fuzzy intrusion event is associated with an attack detection device identification;

the pushing the intrusion event information which is summarized according to the intrusion event types to the security device directed to by the security device identification having a corresponding relationship, so that the security devices adjusts its own defense policy according to the pushed intrusion event information further comprises:

pushing fuzzy intrusion event information to the attack detection device, so that the attack detection device generates an attack source joint detection policy according to the fuzzy intrusion event information, and the attack detection device detects the attack source information according to the attack source joint detection policy.

4. The method according to claim 3, wherein the security device further comprises an attack defense device, and the attack source information is associated with an attack defense device identification;

the pushing the intrusion event information which is summarized according to the intrusion event types to the security device directed to by the security device identification having a

corresponding relationship, so that the security devices adjust its own defense policy according to the pushed intrusion event information further comprises:

pushing the attack source information to the attack defense device, so that the attack defense device generates a joint defense policy according to the attack source information.

40 5. A method for network security joint defense, comprising:

detecting network/system state information and user behavior information in a network/system environment according to an own defense policy to generate security log information;

uploading the generated security log information to a security log sharing platform, wherein the security log sharing platform is configured to classify and summarize the uploaded security log
45 information, to generate a plurality of event types of intrusion event information, and to push the plurality of event types of intrusion event information according to a preset rule;

receiving at least one of the event types of intrusion event information which is pushed by the security log sharing platform; and

generating a joint defense policy by taking the received intrusion event information as clue
50 information.

6. The method according to claim 5, wherein the generating a joint defense policy by taking the received intrusion event information as clue information comprises:

associating the security log information generated by a security device itself with the received intrusion event information to generate joint security log information; and

55 generating a joint defense policy according to the joint security log information, and implementing the joint defense policy to perform intrusion event detection and intrusion event defense.

7. An apparatus for network security joint defense, comprising:

a security log information obtaining module, configured to obtain security log information of a
60 plurality of security devices, wherein the security log information includes intrusion event information violating an own defense policy of the security device, obtained by the security devices in a network/system environment;

a log information classifying module, configured to classify and summarize the intrusion event information included in the security log information according to preset intrusion event types;

65 an associated information obtaining module, configured to obtain a corresponding relationship between each preset intrusion event type and a security device identification; and

a log information pushing module, configured to push the intrusion event information which is summarized according to the intrusion event types to the security device directed to by the security device identification having a corresponding relationship, so that the security device adjusts its own
70 defense policy according to the pushed intrusion event information.

8. The apparatus according to claim 7, wherein further comprising:

a format converting module, configured to convert log formats of the multiple obtained security log information into a preset log format, wherein the preset log format is a log format that is identifiable by the plurality of the security devices.

75 9. The apparatus according to claim 7 or 8, wherein the security device comprises a fuzzy detection device and an attack detection device, the fuzzy detection device is configured to detect a fuzzy intrusion event, the attack detection device is configured to detect attack source information, and the detected fuzzy intrusion event is associated with an attack detection device identification;

80 the log information pushing module is further configured to push fuzzy intrusion event information to the attack detection device, so that the attack detection device generates an attack source joint detection policy according to the fuzzy intrusion event information, and the attack detection device detects the attack source information according to the attack source joint detection policy.

10. An apparatus for network security joint defense, comprising:

85 a security log information generating module, configured to detect network/system state information and user behavior information in a network/system environment according to an own defense policy to generate security log information;

90 a security information sharing module, configured to upload the generated security log information to a security log sharing platform, wherein the security log sharing platform is configured to classify and summarize the uploaded security log information to generate a plurality of event types of intrusion event information, and to push the plurality of event types of intrusion event information according to a preset rule;

an event information receiving module, configured to receive at least one of the event types of intrusion event information which is pushed by the security log sharing platform; and

95 a joint policy generating module, configured to generate a joint defense policy by taking the received intrusion event information as clue information.

11. A server, comprising a memory and a processor, wherein the memory stores computer executable instructions, which, when executed by the processor, cause the processor to perform following steps, comprising:

100 obtaining security log information of a plurality of security devices, wherein the security log information includes intrusion event information violating an own defense policy of the security device obtained by the security device in a network/system environment;

classifying and summarizing the intrusion event information included in the security log information according to preset intrusion event types;

105 obtaining a corresponding relationship between each preset intrusion event type and a security

device identification; and

pushing the intrusion event information which is summarized according to the intrusion event types to the security device directed to by the security device identification having a corresponding relationship, so that the security device adjusts its own defense policy according to the pushed intrusion event information.

12. The server according to claim 11, wherein the processor further performs a following step, comprising: converting log formats of the multiple obtained security log information into a preset log format, wherein the preset log format is a log format that is identifiable by the plurality of the security devices.

13. The server according to claim 11 or 12, wherein the security device comprises a fuzzy detection device and an attack detection device, the fuzzy detection device is configured to detect a fuzzy intrusion event, the attack detection device is configured to detect attack source information, and the detected fuzzy intrusion event is associated with an attack detection device identification;

the processor further performs a following step, comprising:

pushing fuzzy intrusion event information to the attack detection device, so that the attack detection device generates an attack source joint detection policy according to the fuzzy intrusion event information, and the attack detection device detects the attack source information according to the attack source joint detection policy.

14. The server according to claim 13, wherein the security device further comprises an attack defense device, and the attack source information is associated with an attack defense device identification;

the processor further performs a following step, comprising:

pushing the attack source information to the attack defense device, so that the attack defense device generates a joint defense policy according to the attack source information.

15. One or more non-volatile readable storage medium storing computer executable instructions, which, when executed by one or more processors, cause the one or more processors to perform following steps, comprising:

obtaining security log information of a plurality of security devices, wherein the security log information includes intrusion event information violating an own defense policy of the security device obtained by the security device in a network/system environment;

classifying and summarizing the intrusion event information included in the security log information according to preset intrusion event types;

obtaining a corresponding relationship between each preset intrusion event type and a security device identification; and

pushing the intrusion event information which is summarized according to the intrusion event

types to the security device directed to by the security device identification having a corresponding relationship, so that the security device adjusts its own defense policy according to the pushed intrusion event information.

145 16. The non-volatile readable storage medium according to claim 15, wherein the processors further performs a following step, comprising: converting log formats of the multiple obtained security log information into a preset log format, wherein the preset log format is a log format that is identifiable by the plurality of the security devices.

150 17. The non-volatile readable storage medium according to claim 15 or 16, wherein the security device comprises a fuzzy detection device and an attack detection device, the fuzzy detection device is configured to detect a fuzzy intrusion event, the attack detection device is configured to detect attack source information, and the detected fuzzy intrusion event is associated with an attack detection device identification;

the processors further perform a following step, comprising:

155 pushing fuzzy intrusion event information to the attack detection device, so that the attack detection device generates an attack source joint detection policy according to the fuzzy intrusion event information, and the attack detection device detects the attack source information according to the attack source joint detection policy.

160 18. The non-volatile readable storage medium according to claim 17, wherein the security device further comprises an attack defense device, and the attack source information is associated with an attack defense device identification;

the processors further perform a following step, comprising:

pushing the attack source information to the attack defense device, so that the attack defense device generates a joint defense policy according to the attack source information.

165 19. One or more non-volatile readable storage medium storing computer executable instructions, which, when executed by one or more processors, cause the one or more processors to perform following steps, comprising:

detecting network/system state information and user behavior information in a network/system environment according to an own defense policy to generate security log information;

170 uploading the generated security log information to a security log sharing platform, wherein the security log sharing platform is configured to classify and summarize the uploaded security log information, to generate a plurality of event types of intrusion event information, and to push the plurality of event types of intrusion event information according to a preset rule;

receiving at least one of the event types of intrusion event information which is pushed by the security log sharing platform; and

175 generating a joint defense policy by taking the received intrusion event information as clue

information.

20. The non-volatile readable storage medium according to claim 19, wherein the generating a joint defense policy by taking the received intrusion event information as clue information performing by the processors, comprises:

180 associating the security log information generated by a security device itself with the received intrusion event information to generate joint security log information; and

generating a joint defense policy according to the joint security log information, and implementing the joint defense policy to perform intrusion event detection and intrusion event defense.