(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 October 2016 (20.10.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/168044 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 12/26* (2006.01)

(21) International Application Number:
PCT/US2016/026339

(22) International Filing Date:
7 April 2016 (07.04.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/690,302 17 April 2015 (17.04.2015) US

(71) Applicant: CENTRIPETAL NETWORKS, INC. [US/US]; 2251 Corporate Drive, Suite 150, Herndon, Virginia 20171 (US).

(72) Inventors: **AHN, David K.**; c/o Centripetal Networks, Inc., 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171 (US). **GEORGE, Keith A.**; c/o Centripetal Networks, Inc., 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171 (US). **GEREMIA, Peter P.**; c/o Centripetal Networks, Inc., 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171 (US). **MALLETT, III, Pierre**; c/o Centripetal Networks, Inc., 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171 (US). **MOORE, Sean**; c/o Centripetal Networks, Inc., 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171 (US). **PERRY, Robert T.**; c/o Centripetal Networks, Inc., 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171 (US). **ROGERS, Jonathan R.**; c/o Centripetal Networks, Inc., 2251 Corporate Park Drive, Suite 150, Herndon, Virginia 20171 (US).

(74) Agent: **WRIGHT, Bradley**; Suite 1200, 1100 13th Street, NW, Washington, District of Columbia 20005 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: RULE-BASED NETWORK-THREAT DETECTION

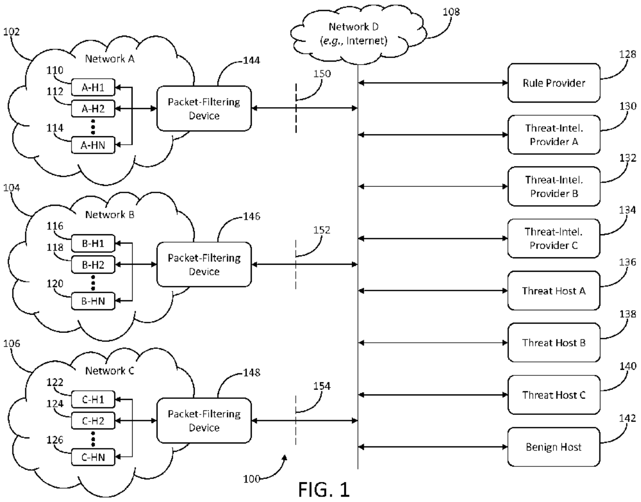


FIG. 1

(57) **Abstract**: A packet-filtering device may receive packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to network-threat indicators. The packet-filtering device may receive packets and, for each packet, may determine that the packet corresponds to criteria specified by a packet-filtering rule. The criteria may correspond to one or more of the network-threat indicators. The packet-filtering device may apply an operator specified by the packet-filtering rule. The operator may be configured to cause the packet-filtering device to either prevent the packet from continuing toward its destination or allow the packet to continue toward its destination. The packet-filtering device may generate a log entry comprising information from the packet-filtering rule that identifies the one or more network-threat indicators and indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

RULE-BASED NETWORK-THREAT DETECTION

CROSS-REFERENCE TO RELATED APPLICATIONS

[01] This application claims priority to U.S. Patent Application Serial No. 14/690,302, filed April 17, 2015, and entitled "RULE-BASED NETWORK-THREAT DETECTION," the disclosure of which is incorporated by reference herein in its entirety and made part hereof.

BACKGROUND

[02] Network security is becoming increasingly important as the information age continues to unfold. Network threats may take a variety of forms (e.g., unauthorized requests or data transfers, viruses, malware, large volumes of network traffic designed to overwhelm network resources, and the like). Many organizations subscribe to network-threat services that periodically provide information associated with network threats, for example, reports that include listings of network-threat indicators (e.g., network addresses, uniform resources identifiers (URIs), and the like). The information provided by such services may be utilized by organizations to identify network threats. For example, logs generated by the organization's network devices may be reviewed for data corresponding to the network-threat indicators provided by such services. But because the logs are generated based on the traffic processed by the network devices without regard to the network-threat indicators, this process is often tedious and time consuming and is exacerbated by the continuously evolving nature of potential threats. Accordingly, there is a need for rule-based network-threat detection.

SUMMARY

[03] The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is intended neither to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts of the disclosure in a simplified form as a prelude to the description below.

[04] Aspects of this disclosure relate to rule-based network-threat detection. In accordance with embodiments of the disclosure, a packet-filtering device may receive packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to network-threat indicators. The packet-filtering device may receive packets and, for each packet, may determine that the packet corresponds to criteria specified by a packet-filtering rule. The criteria may correspond to one or more of the network-threat indicators. The packet-filtering device may apply an operator specified by the packet-filtering rule. The operator may be configured to cause the packet-filtering device to either prevent the packet from continuing toward its destination or allow the packet to continue toward its destination. The packet-filtering device may generate a log entry comprising information from the packet-filtering rule that identifies the one or more network-threat indicators and indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

[05] In some embodiments, the packet-filtering device may generate and communicate to a user device data indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination. The user device may receive the data and indicate in an interface displayed by the user device whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination. The interface may comprise an element that when invoked by a user of the user device causes the user device to instruct the packet-filtering device to reconfigure the operator to prevent future packets corresponding to the criteria from continuing toward their respective destinations.

BRIEF DESCRIPTION OF THE DRAWINGS

[06] The present disclosure is pointed out with particularity in the appended claims. Features of the disclosure will become more apparent upon a review of this disclosure in its entirety, including the drawing figures provided herewith.

[07] Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements, and wherein:

[08] **FIG. 1** depicts an illustrative environment for rule-based network-threat detection in accordance with one or more aspects of the disclosure;

[09] **FIGs. 2A** and **2B** depict illustrative devices for rule-based network-threat detection in accordance with one or more aspects of the disclosure;

[10] **FIGs. 3A**, **3B**, **3C**, **3D**, **3E**, and **3F** depict an illustrative event sequence for rule-based network-threat detection in accordance with one or more aspects of the disclosure;

[11] **FIGs. 4A**, **4B**, and **4C** depict illustrative packet-filtering rules for rule-based network-threat detection in accordance with one or more aspects of the disclosure;

[12] **FIGs. 5A**, **5B**, **5C**, **5D**, **5E**, **5F**, and **5G** depict illustrative logs for rule-based network-threat detection in accordance with one or more aspects of the disclosure;

[13] **FIGs. 6A**, **6B**, **6C**, **6D**, **6E**, **6F**, and **6G** depict illustrative interfaces for rule-based network-threat detection in accordance with one or more aspects of the disclosure; and

[14] **FIG. 7** depicts an illustrative method for rule-based network-threat detection in accordance with one or more aspects of the disclosure.

DETAILED DESCRIPTION

[15] In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the disclosure.

[16] Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless. In this respect, the specification is not intended to be limiting.

[17] **FIG. 1** depicts an illustrative environment for rule-based network-threat detection in accordance with one or more aspects of the disclosure. Referring to **FIG. 1**, environment **100** may include one or more networks. For example, environment **100** may include networks **102**, **104**, **106**, and **108**. Networks **102**, **104**, and **106** may

comprise one or more networks (e.g., Local Area Networks (LANs), Wide Area Networks (WANs), Virtual Private Networks (VPNs), or combinations thereof) associated with one or more individuals or entities (e.g., governments, corporations, service providers, or other organizations). Network **108** may comprise one or more networks (e.g., LANs, WANs, VPNs, or combinations thereof) that interface networks **102**, **104**, and **106** with each other and one or more other networks (not illustrated). For example, network **108** may comprise the Internet, a similar network, or portions thereof.

[18] Environment **100** may also include one or more hosts, such as computing or network devices (e.g., servers, desktop computers, laptop computers, tablet computers, mobile devices, smartphones, routers, gateways, switches, access points, or the like). For example, network **102** may include hosts **110**, **112**, and **114**, network **104** may include hosts **116**, **118**, and **120**, network **106** may include hosts **122**, **124**, and **126**, and network **108** may interface networks **102**, **104**, and **106** with one or more hosts associated with rule provider **128** or network-threat-intelligence providers **130**, **132**, and **134**, threat hosts **136**, **138**, and **140**, and benign host **142**. Network-threat-intelligence providers **130**, **132**, and **134** may be associated with services that monitor network threats (e.g., threats associated with threat hosts **136**, **138**, and **140**) and disseminate (e.g., to subscribers) network-threat-intelligence reports that include network-threat indicators (e.g., network addresses, ports, fully qualified domain names (FQDNs), uniform resource locators (URLs), uniform resource identifiers (URIs), or the like) associated with the network threats, as well as other information associated with the network threats, for example, the type of threat (e.g., phishing malware, botnet malware, or the like), geographic information (e.g., International Traffic in Arms Regulations (ITAR) country, Office of Foreign Assets Control (OFAC) country, or the like), anonymous proxies (e.g., Tor network, or the like), actors (e.g., the Russian Business Network (RBN), or the like).

[19] Environment **100** may further include packet-filtering devices **144**, **146**, and **148**. Packet-filtering device **144** may be located at boundary **150** between networks **102** and **108**. Similarly, packet-filtering device **146** may be located at boundary **152** between networks **104** and **108**, and packet-filtering device **148** may be located at boundary **154** between networks **106** and **108**.

[20] FIGs. **2A** and **2B** depict illustrative devices for rule-based network-threat detection in accordance with one or more aspects of the disclosure.

[21] Referring to FIG. **2A**, as indicated above, packet-filtering device **144** may be located at boundary **150** between networks **102** and **108**. Network **102** may include one or more network devices **202** (e.g., servers, routers, gateways, switches, access points, or the like) that interface hosts **110**, **112**, and **114** with network **108**. Network **102** may also include tap devices **204** and **206**. Tap device **204** may be located on or have access to a communication path that interfaces network devices **202** and network **102** (e.g., one or more of hosts **110**, **112**, and **114**). Tap device **206** may be located on or have access to a communication path that interfaces network devices **202** and network **108**. Packet-filtering device **144** may include memory **208**, one or more processors **210**, one or more communication interfaces **212**, and data bus **214**. Data bus **214** may interface memory **208**, processors **210**, and communication interfaces **212**. Communication interfaces **212** may interface packet-filtering device **144** with network devices **202** and tap devices **204** and **206**. Memory **208** may comprise one or more program modules **216**, one or more packet-filtering rules **218**, and one or more logs **220**. Program modules **216** may comprise instructions that when executed by processors **210** cause packet-filtering device **144** to perform one or more of the functions described herein. Networks **104** and **106** may each comprise components similar to those described herein with respect to network **102**, and packet-filtering devices **146** and **148** may each comprise components similar to those described herein with respect to packet-filtering device **144**.

[22] Referring to **FIG. 2B**, rule provider **128** may include one or more computing devices **222**. Computing devices **222** may include memory **224**, one or more processors **226**, one or more communication interfaces **228**, and data bus **230**. Data bus **230** may interface memory **224**, processors **226**, and communication interfaces **228**. Communication interfaces **228** may interface computing devices **222** with network **108**, which, as indicated above, may interface with network **102** at boundary **150**. Memory **224** may comprise one or more program modules **232**, one or more network-threat indicators **234**, and one or more packet-filtering rules **236**. Program modules **232** may comprise instructions that when executed by processors **226** cause computing devices **222** to perform one or more of the functions described herein.

[23] **FIGs. 3A**, **3B**, **3C**, **3D**, **3E**, and **3F** depict an illustrative event sequence for rule-based network-threat detection in accordance with one or more aspects of the disclosure. In reviewing the illustrative event sequence, it will be appreciated that the number, order, and timing of the illustrative events is simplified for the purpose of illustration and that additional (unillustrated) events may occur, the order and time of events may differ from the depicted illustrative events, and some events or steps may be omitted, combined, or occur in an order other than that depicted by the illustrative event sequence.

[24] Referring to **FIG. 3A**, at step **1**, network-threat-intelligence provider **130** may communicate to rule provider **128** (e.g., via network **108**, as designated by the shaded box over the line extending downward from network **108**) one or more network-threat-intelligence reports identifying one or more network threats (e.g., Threat_1, Threat_2, Threat_3, and Threat_4) and comprising one or more associated network-threat indicators (e.g., network addresses, ports, FQDNs, URLs, URIs, or the like), as well as other information associated with the network threats (e.g., the type of threat, geographic information, anonymous proxies, actors, or the like). Similarly, at step **2**, network-threat-intelligence provider **132** may communicate to rule provider **128** one or more network-threat-intelligence reports identifying one or more network threats (e.g., Threat_1, Threat_2, Threat_5, and Threat_6) and comprising one or more associated network-threat indicators, as well as other information associated with the network threats, and, at step **3**, network-threat-intelligence provider **134** may communicate to rule provider **128** one or more network-threat-intelligence reports identifying one or more network threats (e.g., Threat_1, Threat_7, Threat_8, and Threat_9) and comprising one or more associated network-threat indicators, as well as other information associated with the network threats. Rule provider **128** (e.g., computing devices **222**) may receive (e.g., via communication interfaces **228**) the network-threat-intelligence reports communicated by network-threat-intelligence providers **130**, **132**, and **134**, and may store data contained therein in memory **224** (e.g., network-threat indicators **234**).

[25] Referring to **FIG. 3B**, at step **4**, packet-filtering device **144** may communicate one or more parameters to rule provider **128** (e.g., parameters indicating a preference, authorization, subscription, or the like to receive packet-filtering rules generated based on network-threat-intelligence reports provided by network-threat-intelligence

providers **130**, **132**, and **134**). At step **5**, rule provider **128** (e.g., computing devices **222**) may generate one or more packet-filtering rules (e.g., packet-filtering rules **236**) based on the network-threat-intelligence reports provided by network-threat-intelligence providers **130**, **132**, and **134** (e.g., network-threat indicators **234**) and, at step **6**, may communicate the packet-filtering rules to packet-filtering device **144**, which, at step **7**, may update packet-filtering rules **218** to include the packet-filtering rules generated by rule provider **128** in step **5**.

[26] For example, referring to **FIG. 4A**, packet-filtering rules **218** may include packet-filtering rules **402** that comprise non-network-threat-intelligence rules (e.g., packet-filtering rules generated by an administrator of network **102**) and packet-filtering rules **404** that comprise network-threat-intelligence rules (e.g., the packet-filtering rules communicated by rule provider **128** in step **6**). Each of the network-threat-intelligence rules may comprise: one or more criteria that correspond to one or more of network-threat indicators **234** upon which the rule is based and may be configured to cause packet-filtering device **144** to identify packets corresponding to the criteria (e.g., corresponding to the network-threat indicators upon which the rule is based); an operator configured to cause packet-filtering device **144** to either prevent packets corresponding to the criteria from continuing toward their respective destinations (e.g., a BLOCK operator) or allow packets corresponding to the criteria to continue toward their respective destinations (e.g., an ALLOW operator); and information distinct from the criteria (e.g., a Threat ID) that identifies one or more of the network-threat indicators upon which the rule is based, one or more network threats associated with the network-threat indicators, one or more network-threat-intelligence reports that included the network-threat indicators, one or more of network-threat-intelligence providers **130**, **132**, or **134** that provided the network-threat-intelligence reports, or other information contained in the network-threat-intelligence reports that is associated with the network-threat indicators or the network threats (e.g., the type of threat, geographic information, anonymous proxies, actors, or the like).

[27] Returning to **FIG. 3B**, at step **8**, packet-filtering device **146** may communicate one or more parameters to rule provider **128** (e.g., parameters indicating a preference, authorization, subscription, or the like to receive packet-filtering rules generated based on network-threat-intelligence reports provided by network-threat-intelligence provider **134**). At step **9**, rule provider **128** may generate one or more packet-filtering rules based on the network-threat-intelligence reports provided by network-threat-intelligence provider **134** (e.g., network-threat indicators **234** (or a portion thereof included in network-threat-intelligence reports received from network-threat-intelligence provider **134**)) and, at step **10**, may communicate the packet-filtering rules to packet-filtering device **146**, which, at step **11**, may update its packet-filtering rules to include the packet-filtering rules generated by rule provider **128** in step **9**. Similarly, at step **12**, packet-filtering device **148** may communicate one or more parameters to rule provider **128** (e.g., parameters indicating a preference, authorization, subscription, or the like to receive packet-filtering rules generated based on network-threat-intelligence reports provided by network-threat-intelligence providers **132** and **134**). At step **13**, rule provider **128** may generate one or more packet-filtering rules based on the network-threat-intelligence reports provided by network-threat-intelligence providers **132** and **134** (e.g., network-threat indicators **234** (or a portion thereof included in network-threat-intelligence reports received from network-threat-intelligence providers **132** and **134**)) and, at step **14**, may communicate the packet-filtering rules to packet-filtering device **148**, which, at step **15**, may update its packet-filtering rules to include the packet-filtering rules generated by rule provider **128** in step **13**.

[28] Referring to **FIG. 3C**, at step **16**, four packets may be communicated (e.g., via network **108**, as designated by the shaded circles over the line extending downward from network **108**) between host **114** and benign host **142** (e.g., two packets originating from host **114** and destined for benign host **142** and two packets originating from benign host **142** and destined for host **114**), and packet-filtering device **144** may receive each of the four packets (e.g., via tap devices **204** and **206**), apply one or more of packet-filtering rules **218** to the four packets, and allow the four packets to continue toward their respective destinations.

[29] At step **17**, three packets may be communicated by host **112** to threat host **136**, and packet-filtering device **144** may receive each of the three packets, apply one or more of packet-filtering rules **218** to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule of packet-filtering rules **404** (e.g., Rule: TI003), apply an operator specified by the packet-filtering rule (e.g., an ALLOW operator) to each of the three packets, allow each of the three packets to continue toward its respective destination (e.g., toward threat host **136**), and generate log data for each of the three packets (as designated by the triangles over the line extending downward from packet-filtering device **144**).

[30] At step **18**, packet-filtering device **144** may begin processing the log data generated in step **17**. For example, referring to **FIG. 5A**, logs **220** may include packet log **502** and flow log **504**, each of which (or portions thereof) may be reserved or distinguished for entries associated with packets corresponding to criteria included in packet-filtering rules **404**, and packet-filtering device **144** may generate an entry in packet log **502** for each of the three packets. Each entry may comprise data indicating a hit time for the packet (e.g., a time at which the packet was received by packet-filtering device **144**, identified by packet-filtering device **144**, or the like), data derived from the packet (e.g., a source address, a destination address, a port number, a protocol type, a domain name, URL, URI, or the like), one or more environmental variables (e.g., an identifier of an interface of packet-filtering device **144** over which the packet was received, an identifier of an interface of packet-filtering device **144** over which the packet was forwarded toward its destination, an identifier associated with packet-filtering device **144** (e.g., distinguishing packet-filtering device **144** from packet-filtering devices **146** and **148**), or the like), data identifying the packet-filtering rule of packet-filtering rules **404** to which the packet corresponded (e.g., Thread ID: Threat_3), and data indicating whether packet-filtering device **144** prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination (e.g., the character A may designate that packet-filtering device **144** allowed the packet to continue toward its destination, and the character B may designate that packet-filtering device **144** prevented the packet from continuing toward its destination).

[31] Returning to **FIG. 3C**, at step **19**, four packets may be communicated between host **114** and threat host **138** (e.g., two packets originating from host **114** and destined for threat host **138** and two packets originating from threat host **138** and destined for host **114**), and packet-filtering device **144** may receive each of the four packets, apply one or more of packet-filtering rules **218** to the four packets, determine that each of the four packets corresponds to criteria specified by a packet-filtering rule of packet-filtering rules **404** (e.g., Rule: TI005), apply an operator specified by the packet-filtering rule (e.g., an ALLOW operator) to each of the four packets, allow each of the four packets to continue toward its respective destination, and generate log data for each of the four packets. In some embodiments, the criteria specified by one or more

of packet-filtering rules **404** (e.g., the criteria generated from the network-threat indicators) may include network addresses and one or more of the packets received by packet-filtering device **144** may comprise domain names, URIs, or URLs. In such embodiments, packet-filtering device **144** may comprise a local domain name system (DNS) cache (e.g., stored in memory **208**) and may utilize the local DNS cache to resolve one or more of the domain names, URIs, or URLs included in the packets into one or more of the network addresses included in the criteria.

[32] At step **20**, packet-filtering device **144** may continue processing the log data generated in step **17** and may begin processing the log data generated in step **19**. In some embodiments, packet-filtering device **144** may be configured in accordance with work-conserving scheduling in order to minimize latency (e.g., the time between when a packet corresponding to a network threat crosses boundary **150** and the time when an administrator associated with network **102** is presented with an interface indicating that the packet corresponding to the network threat has crossed boundary **150**). For example, referring to **FIG. 5B**, packet-filtering device **144** may generate entries in packet log **502** for each of the packets received in step **19** while generating an entry in flow log **504** for the packets received in step **17**. Packet-filtering device **144** may generate the entry in flow log **504** for the packets received in step **17** based on the entries generated in packet log **502** (e.g., in step **18**) for the packets received in step **17**. The entry in flow log **504** may consolidate, compress, or summarize the entries in packet log **502**. For example, the entry in flow log **504** may comprise a time range (e.g., [01, 03]) indicating the earliest hit time indicated by the entries (e.g., Time: 01) to the latest hit time indicated by the entries (e.g., Time: 03), consolidated information from the entries (e.g., a consolidation of the information derived from the packets and the environmental variables), information that each of the associated packets have in common (e.g., Threat ID: Threat_3), a count of the associated packets allowed by packet-filtering device **144** to continue toward their respective destinations, and a count of the associated packets prevented by packet-filtering device **144** from continuing toward their respective destinations.

[33] Returning to **FIG. 3C**, at step **21**, packet-filtering device **144** may utilize flow log **504** to generate data comprising an update for an interface associated with packet-filtering device **144** and displayed by host **110**, and may communicate the data comprising the update to host **110**. For example, referring to **FIG. 6A**, host **110** may be a user device associated with an administrator of network **102** and configured to display interface **600**. Interface **600** may include graphical depictions **602** and **604**, which may illustrate activity associated with packet-filtering device **144**. For example, graphical depiction **602** may comprise a line chart depicting, for a user-specified time interval, a number of packet hits, a number of packets prevented from continuing toward their respective destinations, a number of packets allowed to continue toward their respective destinations, or the like, and graphical depiction **604** may comprise an annulated pie chart illustrating percentages of hits during the user-specified time interval that are associated with various category types (e.g., type of network threat, geographic information, anonymous proxies, actors, or the like).

[34] Interface **600** may also include listing **606**, which may comprise entries corresponding to network threats and, for each threat, associated information derived by packet-filtering device **144** from flow log **504** (e.g., a description of the threat, information derived from the consolidated information stored in flow log **504**, the time of the last associated packet hit, a count of associated packet hits, a count of associated packets allowed by packet-filtering device **144** to continue toward their respective destinations, a count of associated packets prevented by packet-filtering device **144** from continuing toward their respective destinations) and a status of the operator included in the rule associated with the threat.

[35] Packet-filtering device **144** may be configured to determine an ordering of the network threats, and listing **606** may be displayed in accordance with the ordering determined by packet-filtering device **144**. In some embodiments, packet-filtering device **144** may be configured to determine a score for each of the network threats and the ordering may be determined based on the scores. In such embodiments, the scores may be determined based on a number of associated packet hits, times associated with the packet hits (e.g., time of day, time since last hit, or the like), whether the packet was destined for a network address associated with a host in network **102** or a host in network **108**, one or more network-threat-intelligence providers that provided the network-threat indicators associated with the threat, the number of network-threat intelligence providers that provided the network-threat indicators associated with the threat, other information associated with the network threat (e.g., type of network threat, geographic information, anonymous proxies, actors, or the like).

[36] For example, as illustrated in **FIG. 6A**, the threat associated with Threat ID: Threat_1 may be assigned a score (e.g., 6) higher than the score assigned to the threat associated with Threat ID: Threat_2 (e.g., 5) based on a determination that the network-threat-indicators corresponding to the threat associated with Threat ID: Threat_1 were received from three different network-threat-intelligence providers (e.g., network-threat-intelligence providers **130**, **132**, and **134**) and a determination that the network-threat-indicators corresponding to the threat associated with Threat ID: Threat_2 were received from two different network-threat-intelligence providers (e.g., network-threat-intelligence providers **130** and **132**). Similarly, the threat associated with Threat ID: Threat_2 may be assigned a score (e.g., 5) higher than the score assigned to the threat associated with Threat ID: Threat_3 (e.g., 4) based on a determination that the network-threat-indicators corresponding to the threat associated with Threat ID: Threat_2 were received from two different network-threat-intelligence providers (e.g., network-threat-intelligence providers **130** and **132**) and a determination that the network-threat-indicators corresponding to the threat associated with Threat ID: Threat_3 were received from one network-threat-intelligence provider (e.g., network-threat-intelligence provider **130**). Additionally, the threat associated with Threat ID: Threat_3 may be assigned a score (e.g., 4) higher than the score assigned to the threat associated with Threat ID: Threat_5 (e.g., 2) based on a determination that the last packet hit corresponding to the threat associated with Threat ID: Threat_3 is more recent than the last packet hit corresponding to the threat associated with Threat ID: Threat_5, and the threat associated with Threat ID: Threat_4 may be assigned a score (e.g., 2) higher than the score assigned to the threat associated with Threat ID: Threat_9 (e.g., 1) based on a determination that the network-threat-indicators corresponding to the threat associated with Threat ID: Threat_4 were received from network-threat-intelligence provider **130** and a determination that the network-threat-indicators corresponding to the threat associated with Threat ID: Threat_9 were received from network-threat-intelligence provider **134** (e.g., the network-threat-intelligence reports produced by network-threat-intelligence provider **130** may be regarded as more reliable than the network-threat-intelligence reports produced by network-threat-intelligence provider **134**).

[37] Returning to **FIG. 3C**, at step **22**, three packets may be communicated by threat host **140** to host **114**, and packet-filtering device **144** may receive each of the three

packets, apply one or more of packet-filtering rules **218** to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule of packet-filtering rules **404** (e.g., Rule: TI001), apply an operator specified by the packet-filtering rule (e.g., an ALLOW operator) to each of the three packets, allow each of the three packets to continue toward its respective destination (e.g., toward host **114**), and generate log data for each of the three packets.

[38] At step **23**, packet-filtering device **144** may continue processing the log data generated in step **19** and may begin processing the log data generated in step **22**. For example, referring to **FIG. 5C**, packet-filtering device **144** may generate entries in packet log **502** for each of the packets received in step **22** while generating an entry in flow log **504** for the packets received in step **19** based on the entries generated in packet log **502** (e.g., in step **20**) for the packets received in step **19**.

[39] Returning to **FIG. 3C**, at step **24**, packet-filtering device **144** may utilize flow log **504** to generate data comprising an update for interface **600** and may communicate the data to host **110**. For example, referring to **FIG. 6B**, the update may cause interface **600** to update an entry in listing **606** corresponding to the threat associated with Threat ID: Threat_5 to reflect the packets received in step **19** and to reflect a new score (e.g., 3) assigned by packet-filtering device **144** to the threat associated with Threat ID: Threat_5 (e.g., the score may have increased based on the packets received in step **19**).

[40] Interface **600** may include one or more block options that when invoked by a user of host **110** (e.g., the administrator of network **102**) cause host **110** to instruct packet-filtering device **144** to reconfigure an operator of a packet-filtering rule included in packet-filtering rules **404** to prevent packets corresponding to the criteria specified by the packet-filtering rule from continuing toward their respective destinations. In some embodiments, listing **606** may include such a block option alongside each entry, and, when invoked, the block option may cause host **110** to instruct packet-filtering device **144** to reconfigure an operator of packet-filtering rules **404** that corresponds to the network threat associated with the entry. For example, interface **600** may include block option **608**, which, when invoked, may cause host **110** to instruct packet-filtering device **144** to reconfigure an operator associated with Rule: TI003 (e.g., to reconfigure the operator to cause packet-filtering device **144** to prevent packets corresponding to the one or more criteria specified by Rule: TI003 (e.g., packets corresponding to the network-threat-indicators associated with Threat ID: Threat_3) from continuing toward their respective destinations).

[41] Additionally or alternatively, when invoked, such a block option may cause host **110** to display another interface (e.g., an overlay, pop-up interface, or the like) associated with packet-filtering device **144**. For example, referring to **FIG. 6C**, when invoked, block option **608** may cause host **110** to display interface **610**. Interface **610** may comprise specific block options **612**, **614**, **616**, and **618**, modify option **620**, and cancel option **622**. Specific block option **612** may correspond to an option to reconfigure packet-filtering device **144** to prevent packets corresponding to the network threat and destined for or originating from a host in network **102** from continuing toward their respective destinations. Specific block option **614** may correspond to an option to reconfigure packet-filtering device **144** to prevent packets corresponding to the network threat and destined for or originating from one or more particular hosts in network **102** that have generated or received packets associated with the network threat (e.g., host **112**) from continuing toward their respective destinations. Specific block option **616** may correspond to an option to reconfigure packet-filtering device **144** to prevent any packets received from the particular hosts in network **102** that have generated or received packets associated with the network threat from continuing toward hosts located in network **102**. And specific block option **618** may correspond to an option to reconfigure packet-filtering device **144** to prevent any packets received from the particular hosts in network **102** that have generated or received packets associated with the network threat from continuing toward hosts located in network **108**.

[42] Interface **610** may also include rule-preview listing **624**, which may display a listing of rules that will be implemented by packet-filtering device **144** in response to the user invoking modify option **620**. Rule-preview listing **624** may include one or more entries corresponding to each of specific block options **612**, **614**, **616**, and **618**. For example, entry **626** may correspond to, and display a rule configured to implement, specific block option **612** (e.g., Rule: TI003 with its operator reconfigured to BLOCK). Similarly, entries **628**, **630**, and **632** may correspond to, and display rules configured to implement, specific block options **614**, **616**, and **618** (e.g., one or more new rules generated by packet-filtering device **144** based on data derived from flow log **504** (e.g., a network address associated with host **112**)). Responsive to a user invoking one or more of specific block options **612**, **614**, **616**, or **618**, the interface may select the corresponding rules, and responsive to a user invoking modify option **620**, host **110** may instruct packet-filtering device **144** to implement the selected rules. Responsive to a user invoking cancel option **620**, host **110** may redisplay interface **600**.

[43] Returning to **FIG. 3C**, at step **25**, host **110** may communicate instructions to packet-filtering device **144** instructing packet-filtering device **144** to reconfigure one or more of packet-filtering rules **404** (e.g., to reconfigure the operator of Rule: TI003 to BLOCK), and, at step **26**, packet-filtering device **144** may reconfigure packet-filtering rules **404** accordingly, as reflected in **FIG. 4B**.

[44] At step **27**, three packets destined for threat host **136** may be communicated by host **112**, and packet-filtering device **144** may receive each of the three packets, apply one or more of packet-filtering rules **218** to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule of packet-filtering rules **404** (e.g., Rule: TI003), apply an operator specified by the packet-filtering rule (e.g., the BLOCK operator) to each of the three packets, prevent each of the three packets from continuing toward its respective destination (e.g., toward threat host **136**), and generate log data for each of the three packets.

[45] At step **28**, packet-filtering device **144** may continue processing the log data generated in step **22** and may begin processing the log data generated in step **27**. For example, referring to **FIG. 5D**, packet-filtering device **144** may generate entries in packet log **502** for each of the packets received in step **27** while generating an entry in flow log **504** for the packets received in step **22** based on the entries generated in packet log **502** (e.g., in step **23**) for the packets received in step **22**.

[46] Returning to **FIG. 3C**, at step **29**, packet-filtering device **144** may utilize flow log **504** to generate data comprising an update for interface **600** and may communicate the data to host **110**. For example, referring to **FIG. 6D**, the update may cause interface **600** to update an entry in listing 606 that is associated with the threat associated with Threat ID: Threat_1 to reflect the packets received in step **22**, the change in the operator of the packet-filtering rule associated with the threat associated with Thread ID: Threat_3, a new score (e.g., 7) assigned by packet-filtering device **144** to the threat associated with Threat ID: Threat_1 (e.g., the score may have increased based

on the packets received in step **22**), a new score (e.g., 2) assigned by packet-filtering device **144** to the threat associated with Threat ID: Threat_3 (e.g., the score may have decreased based on the change of the operator in its associated packet-filtering rule), a new score (e.g., 4) assigned by packet-filtering device **144** to the threat associated with Threat ID: Threat_5, and a revised ordering, determined by packet-filtering device **144** based on the new scores.

[47] Referring to **FIG. 3D**, at step **30**, three packets destined for host **120** may be communicated by threat host **140**, and packet-filtering device **146** may receive each of the three packets, apply one or more of its packet-filtering rules to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule (e.g., a rule corresponding to Threat ID: Threat_1), apply an operator specified by the packet-filtering rule (e.g., an ALLOW operator) to each of the three packets, allow each of the three packets to continue toward its respective destination (e.g., toward host **120**), and generate log data for each of the three packets. At step **31**, packet-filtering device **146** may begin processing the log data generated in step **30**.

[48] At step **32**, three packets destined for host **118** may be communicated by threat host **140**, and packet-filtering device **146** may receive each of the three packets, apply one or more of its packet-filtering rules to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule (e.g., the rule corresponding to Threat ID: Threat_1), apply an operator specified by the packet-filtering rule (e.g., an ALLOW operator) to each of the three packets, allow each of the three packets to continue toward its respective destination (e.g., toward host **118**), and generate log data for each of the three packets.

[49] At step **33**, packet-filtering device **146** may continue processing the log data generated in step **30** and may begin processing the log data generated in step **33**. At step **34**, packet-filtering device **146** may generate data comprising an update for an interface associated with packet-filtering device **146** and displayed by host **116** (e.g., an interface similar to interface **600**) and may communicate the data comprising the update to host **116**.

[50] At step **35**, three packets destined for host **120** may be communicated by threat host **140**, and packet-filtering device **146** may receive each of the three packets, apply one or more of its packet-filtering rules to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule (e.g., the rule corresponding to Threat ID: Threat_1), apply an operator specified by the packet-filtering rule (e.g., an ALLOW operator) to each of the three packets, allow each of the three packets to continue toward its respective destination (e.g., toward host **120**), and generate log data for each of the three packets. At step **36**, packet-filtering device **146** may continue processing the log data generated in step **32** and may begin processing the log data generated in step **35**.

[51] At step **37**, packet-filtering device **146** may generate data comprising an update for the interface associated with packet-filtering device **146** and displayed by host **116** and may communicate the data comprising the update to host **116**. At step **38**, host **116** may communicate instructions to packet-filtering device **146** instructing packet-filtering device **146** to reconfigure one or more of its packet-filtering rules (e.g., to reconfigure the operator of the rule corresponding to Threat ID: Threat_1 to BLOCK), and, at step **39**, packet-filtering device **146** may reconfigure its packet-filtering rules accordingly.

[52] At step **40**, three packets destined for host **118** and three packets destined for host **120** may be communicated by threat host **140**, and packet-filtering device **146** may receive each of the six packets, apply one or more of its packet-filtering rules to the six packets, determine that each of the six packets corresponds to criteria specified by a packet-filtering rule (e.g., the rule corresponding to Threat ID: Threat_1), apply an operator specified by the packet-filtering rule (e.g., the BLOCK operator) to each of the six packets, prevent each of the six packets from continuing toward its respective destination, and generate log data for each of the six packets. At step **41**, packet-filtering device **146** may continue processing the log data generated in step **35** and may begin processing the log data generated in step **40**.

[53] At step **42**, packet-filtering device **146** may communicate data to rule provider **128** (e.g., data indicating that fifteen packets corresponding to Threat ID: Threat_1 were received by packet-filtering device **146**, packet-filtering device **146** allowed nine of the fifteen packets to continue toward hosts in network **104**, and packet-filtering device **146** prevented six of the fifteen packets from continuing toward hosts in network **104**).

[54] Referring to **FIG. 3E**, at step **43**, four packets may be communicated between host **124** and threat host **136** (e.g., two packets originating from host **124** and destined for threat host **136** and two packets originating from threat host **136** and destined for host **124**), and packet-filtering device **148** may receive each of the four packets, apply one or more of its packet-filtering rules to the four packets, and allow the four packets to continue toward their respective destinations.

[55] At step **44**, three packets destined for host **126** may be communicated by threat host **140**, and packet-filtering device **148** may receive each of the three packets, apply one or more of its packet-filtering rules to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule (e.g., a rule corresponding to Threat ID: Threat_1), apply an operator specified by the packet-filtering rule (e.g., an ALLOW operator) to each of the three packets, allow each of the three packets to continue toward its respective destination (e.g., toward host **126**), and generate log data for each of the three packets. At step **45**, packet-filtering device **148** may begin processing the log data generated in step **44**.

[56] At step **46**, three packets destined for host **126** may be communicated by threat host **140**, and packet-filtering device **148** may receive each of the three packets, apply one or more of its packet-filtering rules to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule (e.g., the rule corresponding to Threat ID: Threat_1), apply an operator specified by the packet-filtering rule (e.g., an ALLOW operator) to each of the three packets, allow each of the three packets to continue toward its respective destination (e.g., toward host **126**), and generate log data for each of the three packets.

[57] At step **47**, packet-filtering device **148** may continue processing the log data generated in step **44** and may begin processing the log data generated in step **47**. At step **48**, packet-filtering device **148** may generate data comprising an update for an interface associated with packet-filtering device **148** and displayed by host **122** (e.g., an interface similar to interface **600**) and may communicate the data comprising the update to host **122**.

[58] At step **49**, two packets may be communicated between host **124** and threat host **138** (e.g., a packet originating from host **124** and destined for threat host **138** and a packet originating from threat host **138** and destined for host **124**), and packet-filtering

device **148** may receive each of the two packets, apply one or more of its packet-filtering rules to the two packets, determine that each of the two packets corresponds to criteria specified by a packet-filtering rule (e.g., a rule corresponding to Threat ID: Threat_5), apply an operator specified by the packet-filtering rule (e.g., an ALLOW operator) to each of the two packets, allow each of the two packets to continue toward its respective destination, and generate log data for each of the two packets. At step **50**, packet-filtering device **148** may continue processing the log data generated in step **46** and may begin processing the log data generated in step **49**.

[59] At step **51**, packet-filtering device **148** may generate data comprising an update for the interface associated with packet-filtering device **148** and displayed by host **122** and may communicate the data comprising the update to host **122**. At step **52**, host **122** may communicate instructions to packet-filtering device **148** instructing packet-filtering device **148** to reconfigure one or more of its packet-filtering rules to block all packets corresponding to the network-threat indicators associated with Threat ID: Threat_1 (e.g., to reconfigure the operator of the rule corresponding to Threat ID: Threat_1 to BLOCK), and to implement one or more new packet-filtering rules configured to block all packets originating from host **126**, and, at step **53**, packet-filtering device **148** may reconfigure its packet-filtering rules accordingly.

[60] At step **54**, threat host **140** may generate a packet destined for host **124** and a packet destined for host **126**, host **126** may generate a packet destined for benign host **142** and a packet destined for host **124**, and packet-filtering device **148** may receive each of the four packets, apply one or more of its packet-filtering rules to the four packets, determine that the packets generated by threat host **140** correspond to criteria specified by the packet-filtering rule corresponding to Threat ID: Threat_1, apply an operator specified by the packet-filtering rule corresponding to Threat ID: Threat_1 (e.g., the BLOCK operator) to each of the two packets generated by threat host **140**, determine that the packets generated by host **126** correspond to criteria specified by the new packet-filtering rules (e.g., a network address associated with host **126**), apply an operator specified by the new packet-filtering rules (e.g., the BLOCK operator) to each of the two packets generated by host **126**, prevent each of the four packets from continuing toward its respective destination, and generate log data for each of the four packets.

[61] At step **55**, packet-filtering device **148** may continue processing the log data generated in step **49** and may begin processing the log data generated in step **54**. At step **56**, packet-filtering device **148** may communicate data to rule provider **128** (e.g., data indicating that eight packets corresponding to Threat ID: Threat_1 were received by packet-filtering device **148**, packet-filtering device **148** allowed six of the eight packets to continue toward hosts in network **106**, packet-filtering device **148** prevented two of the eight packets from continuing toward hosts in network **106**, two packets corresponding to Threat ID: Threat_5 were received by packet-filtering device **148**, and packet-filtering device **148** allowed both of the two packets to continue toward their respective destinations).

[62] Referring to **FIG. 3F**, at step **57**, rule provider **128** (e.g., computing devices **222**) may analyze the data received from packet-filtering devices **146** and **148** (e.g., in steps **42** and **56**, respectively) and may generate, based on the analysis, an update for packet-filtering device **148**. In some embodiments, the update may be configured to cause packet-filtering device **144** to reconfigure an operator of a packet-filtering rule included in packet-filtering rules **404** (e.g., to reconfigure packet-filtering device **144** to prevent packets corresponding to the criteria specified by the rule from continuing toward their respective destinations). Additionally or alternatively, the update may reconfigure one or more of packet-filtering rules **404** to affect the ordering (e.g., the scoring) of the network threats associated with packet-filtering rules **404**. At step **58**, rule provider **128** may communicate the updates to packet-filtering device **144**, which may receive the updates and, at step **59**, may update packet-filtering rules **404** accordingly. For example, the update may be configured to cause packet-filtering device **144** to reconfigure the operator of Rule: TI001 to the BLOCK operator (e.g., to reconfigure packet-filtering device **144** to prevent packets corresponding to the network-threat indicators associated with the network threat corresponding to Threat ID: Threat_1 from continuing toward their respective destinations, and packet-filtering device **144** may reconfigure packet-filtering rules **404** accordingly, as reflected in **FIG. 4C**).

[63] At step **60**, four packets may be communicated between host **114** and benign host **142** (e.g., two packets originating from host **114** and destined for benign host **142** and two packets originating from benign host **142** and destined for host **114**), and packet-filtering device **144** may receive each of the four packets, apply one or more of

packet-filtering rules **218** to the four packets, and allow the four packets to continue toward their respective destinations.

[64] At step **61**, three packets destined for threat host **136** may be communicated by host **112**, and packet-filtering device **144** may receive each of the three packets, apply one or more of packet-filtering rules **218** to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule of packet-filtering rules **404** (e.g., Rule: TI003), apply an operator specified by the packet-filtering rule (e.g., the BLOCK operator) to each of the three packets, prevent each of the three packets from continuing toward its respective destination (e.g., toward threat host **136**), and generate log data for each of the three packets.

[65] At step **62**, packet-filtering device **144** may continue processing the log data generated in step **27** and may begin processing the log data generated in step **62**. For example, referring to **FIG. 5E**, packet-filtering device **144** may generate entries in packet log **502** for each of the packets received in step **61** while modifying an entry in flow log **504** for the packets received in step **27** based on the entries generated in packet log **502** (e.g., in step **28**) for the packets received in step **27**, for example, modifying the entry corresponding to Threat ID: Threat_3) (e.g., the time range and the count of associated packets prevented by packet-filtering device **144** from continuing toward their respective destinations).

[66] At step **63**, packet-filtering device **144** may utilize flow log **504** to generate data comprising an update for interface **600** and may communicate the data to host **110**. For example, referring to **FIG. 6E**, the update may cause interface **600** to update the entry in listing **606** associated with Threat ID: Threat_3 to reflect the packets received in step **27**, the change in the operator of the packet-filtering rule associated with Thread ID: Threat_1, a new score (e.g., 3) assigned by packet-filtering device **144** to the threat associated with Threat ID: Threat_3 (e.g., the score may have increased based on the packets received in step **27**), and a new score (e.g., 5) assigned by packet-filtering device **144** to the threat associated with Threat ID: Threat_1 (e.g., the score may have decreased based on the change of the operator in its associated packet-filtering rule).

[67] At step **64**, three packets destined for host **112** and three packets destined for host **114** may be communicated by threat host **140**, and packet-filtering device **144** may receive each of the six packets, apply one or more of packet-filtering rules **218** to the three packets, determine that each of the three packets corresponds to criteria specified by a packet-filtering rule of packet-filtering rules **404** (e.g., Rule: TI001), apply an operator specified by the packet-filtering rule (e.g., the BLOCK operator) to each of the six packets, prevent each of the six packets from continuing toward its respective destination, and generate log data for each of the six packets.

[68] At step **65**, packet-filtering device **144** may continue processing the log data generated in step **61** and may begin processing the log data generated in step **64**. For example, referring to **FIG. 5F**, packet-filtering device **144** may generate entries in packet log **502** for each of the packets received in step **64** while modifying an entry in flow log **504** for the packets received in step **61** based on the entries generated in packet log **502** (e.g., in step **62**) for the packets received in step **61**, for example, modifying the entry corresponding to Threat ID: Threat_3 (e.g., the time range and the count of associated packets prevented by packet-filtering device **144** from continuing toward their respective destinations).

[69] At step **66**, packet-filtering device **144** may utilize flow log **504** to generate data comprising an update for interface **600** and may communicate the data to host **110**. For example, referring to **FIG. 6F**, the update may cause interface **600** to update the entry in listing **606** associated with Threat ID: Threat_3 to reflect the packets received in step **61** and a new score (e.g., 3) assigned by packet-filtering device **144** to the threat associated with Threat ID: Threat_3 (e.g., the score may have increased based on the packets received in step **61**).

[70] At step **67**, packet-filtering device **144** may continue processing the log data generated in step **64**. For example, referring to **FIG. 5G**, packet-filtering device **144** may modify an entry in flow log **504** for the packets received in step **64** based on the entries generated in packet log **502** (e.g., in step **65**) for the packets received in step **64**, for example, modifying the entry corresponding to Threat ID: Threat_1 (e.g., the time range and the count of associated packets prevented by packet-filtering device **144** from continuing toward their respective destinations).

[71] At step **68**, packet-filtering device **144** may utilize flow log **504** to generate data comprising an update for interface **600** and may communicate the data to host **110**. For example, referring to FIG. **6G**, the update may cause interface **600** to update the entry in listing **606** associated with Threat ID: Threat_1 to reflect the packets received in step **64** and a new score (e.g., 6) assigned by packet-filtering device **144** to the threat associated with Threat ID: Threat_1 (e.g., the score may have increased based on the packets received in step **64**).

[72] **FIG. 7** depicts an illustrative method for rule-based network-threat detection in accordance with one or more aspects of the disclosure. Referring to **FIG. 7**, at step **702**, a packet-filtering device may receive a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to one or more network-threat indicators. For example, packet-filtering device **144** may receive packet-filtering rules **404** from rule provider **128**. At step **704**, the packet-filtering device may receive a packet corresponding to at least one of the network-threat indicators. For example, packet-filtering device **144** may receive a packet generated by host **112** and destined for threat host **136**. At step **706**, the packet-filtering device may determine that the packet corresponds to criteria specified by one of the plurality of packet-filtering rules. For example, packet-filtering device **144** may determine that the packet generated by host **112** and destined for threat host **136** corresponds to Rule: TI003. At step **708**, the packet-filtering device may apply an operator specified by the packet-filtering rule to the packet. For example, packet-filtering device **144** may apply an operator (e.g., an ALLOW operator) specified by Rule: TI003 to the packet generated by host **112** and may allow the packet generated by host **112** to continue toward threat host **136**.

[73] At step **710**, the packet-filtering device may generate a log entry comprising information from the packet-filtering rule that is distinct from the criteria and identifies the one or more network-threat indicators. For example, packet-filtering device **144** may generate an entry in packet log **502** comprising Threat ID: Threat_3 for the packet generated by host **112**. At step **712**, the packet-filtering device may generate data indicating whether the packet-filtering device prevented the packet from continuing toward its destination (e.g., blocked the packet) or allowed the packet to continue toward its destination. For example, packet-filtering device **144** may generate data comprising an update for interface **600** that indicates that packet-filtering device **144** allowed the packet generated by host **112** to continue toward threat host **136**. At step **714**, the packet-filtering device may communicate the data to a user device. For example, packet-filtering device **144** may communicate the data

comprising the update for interface **600** to host **110**. At step **716**, the packet-filtering device may indicate in an interface whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination. For example, communicating the data comprising the update for interface **600** may cause host **110** to indicate in interface **600** that packet-filtering device **144** allowed the packet generated by host **112** to continue toward threat host **136**.

[74] The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data-processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer-executable instructions and computer-usable data described herein.

[75] Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, system, apparatus, or one or more computer-readable media storing computer-executable instructions. Accordingly, aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

[76] As described herein, the various methods and acts may be operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device (e.g., a server, client computer, or the like).

[77] Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order and that one or more illustrated steps may be optional. Any and all features in the following claims may be combined or rearranged in any way possible.

CLAIMS

What is claimed is:

1. A method comprising:

receiving, by a packet-filtering device, a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;

receiving, by the packet-filtering device, a plurality of packets; and

for each packet of the plurality of packets and responsive to a determination by the packet-filtering device that the packet corresponds to one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators:

applying, by the packet-filtering device and to the packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to either prevent the packet from continuing toward its destination or allow the packet to continue toward its destination;

generating, by the packet-filtering device, a packet-log entry comprising information from the packet-filtering rule that identifies the one or more network-threat indicators and indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination;

generating, by the packet-filtering device and based on the packet-log entry, data indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination;

communicating, by the packet-filtering device and to a user device, the data; and

indicating, based on the data, in an interface displayed by the user device, and in a portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators, whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

2. The method of claim 1, wherein the plurality of packets comprises a first packet and a second packet, and wherein both the first packet and the second packet correspond to one or more particular criteria, specified by a particular packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more particular network-threat indicators of the plurality of network-threat indicators, the method comprising:

responsive to a determination by the packet-filtering device that the first packet corresponds to the one or more particular criteria, allowing, by the packet-filtering device, the first packet to continue toward its destination; and

responsive to a determination by the packet-filtering device that the second packet corresponds to the one or more particular criteria, preventing, by the packet-filtering device, the second packet from continuing toward its destination.

3. The method of claim 2, comprising modifying, by the packet-filtering device, after the determination by the packet-filtering device that the first packet corresponds to the one or more particular criteria, before the determination by the packet-filtering device that the second packet corresponds to the one or more particular criteria, and responsive to an instruction received from the user device, an operator specified by the particular packet-filtering rule to reconfigure the packet-filtering device to prevent packets corresponding to the one or more particular criteria from continuing toward their respective destinations.

4. The method of claim 2, wherein:

the packet-filtering device is located at a boundary between a first network and a second network;

both the first packet and the second packet are received from a common host in the first network and destined for a common host in the second network;

the determination by the packet-filtering device that the first packet corresponds to the one or more particular criteria comprises a determination that the first packet was received from the common host in the first network;

the determination by the packet-filtering device that the second packet corresponds to the one or more particular criteria comprises a determination that the second packet was received from the common host in the first network;

allowing the first packet to continue toward its destination comprises allowing the first packet to continue toward the common host in the second network; and preventing the second packet from continuing toward its destination comprises preventing the second packet from continuing toward the common host in the second network.

5. The method of claim 2, wherein:

the packet-filtering device is located at a boundary between a first network and a second network;

both the first packet and the second packet are received from a common host in the first network;

the first packet is destined for a first host in the second network;

the second packet is destined for a second host in the second network;

the determination by the packet-filtering device that the first packet corresponds to the one or more particular criteria comprises a determination that the first packet was received from the common host;

the determination by the packet-filtering device that the second packet corresponds to the one or more particular criteria comprises a determination that the second packet was received from the common host;

allowing the first packet to continue toward its destination comprises allowing the first packet to continue toward the first host; and

preventing the second packet from continuing toward its destination comprises preventing the second packet from continuing toward the second host.

6. The method of claim 2, wherein:

the packet-filtering device is located at a boundary between a first network and a second network;

both the first packet and the second packet are destined for a common host in the first network;

the first packet is received from a first host in the second network;

the second packet is received from a second host in the second network;

the determination by the packet-filtering device that the first packet corresponds to the one or more particular criteria comprises a determination that the first packet is destined for the common host;

the determination by the packet-filtering device that the second packet corresponds to the one or more particular criteria comprises a determination that the second packet is destined for the common host;

allowing the first packet to continue toward its destination comprises allowing the first packet to continue toward the common host; and

preventing the second packet from continuing toward its destination comprises preventing the second packet from continuing toward the common host.

7. The method of claim 1, comprising, for each packet of the plurality of packets and responsive to the determination by the packet-filtering device that the packet corresponds to the one or more criteria, updating, by the packet-filtering device and based on the packet-log entry, a packet-flow log to indicate the determination and whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

8. The method of claim 7, wherein receiving the plurality of packets comprises receiving a first portion of packets and a second portion of packets, the method comprising:

for each packet in the first portion of packets:

generating, by the packet-filtering device, a packet-log entry indicating one or more particular network-threat indicators of the plurality of network-threat indicators to which the packet corresponds and whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination; and

generating, by the packet-filtering device and based on the packet-log entry, a flow-log entry indicating the one or more particular network-threat indicators and whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination; and

for each packet in the second portion of packets:

generating, by the packet-filtering device, a packet-log entry indicating one or more particular network-threat indicators of the plurality of network-threat indicators to which the packet corresponds and whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination; and modifying, by the packet-filtering device and based on the packet-log entry, an existing flow-log entry corresponding to the one or more particular network-threat indicators to reflect whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

9. The method of claim 8, wherein:

the second portion of packets is received by the packet-filtering device after the first portion of packets is received by the packet-filtering device; and

for each packet in the second portion of packets, generating the packet-log entry comprises generating the packet-log entry while the packet-filtering device is generating one or more flow-log entries for one or more packets in the first portion of packets.

10. The method of claim 9, comprising:

receiving, by the packet-filtering device and after receiving the second portion of packets, a third portion of packets; and

generating, by the packet-filtering device, for each packet in the third portion of packets, and while modifying one or more existing flow-log entries based on one or more packet-log entries generated for one or more packets in the second portion, a packet-log entry for the packet.

11. The method of claim 1, wherein:

each of the plurality of network-threat indicators corresponds to at least one network threat of a plurality of network threats;

each of the plurality of packet-filtering rules corresponds to a different network threat of the plurality of network threats; and

generating the packet-log entry comprises generating a packet-log entry identifying a particular network threat of the plurality of network threats to which the packet corresponds.

12. The method of claim 11, comprising, for each packet of the plurality of packets and responsive to the determination by the packet-filtering device that the packet corresponds to the one or more criteria that correspond to the one or more network-threat indicators, updating, by the packet-filtering device and based on the packet-log entry, a packet-flow log to indicate the determination and whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

13. The method of claim 12, wherein:

the packet-flow log comprises a plurality of packet-flow-log entries;

each packet-flow-log entry of the plurality of packet-flow-log entries corresponds to a different network threat of the plurality of network threats;

the one or more network-threat indicators correspond to the particular network threat; and

updating the packet-flow log comprises updating a packet-flow-log entry, of the plurality of packet-flow-log entries, that corresponds to the particular network threat.

14. The method of claim 13, wherein generating the data indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination comprises generating the data based on the packet-flow-log entry that corresponds to the particular network threat.

15. The method of claim 14, wherein:

the interface comprises a plurality of different portions;

each portion of the plurality of different portions corresponds to a different packet-filtering rule of the plurality of packet-filtering rules and a different network threat of the plurality of network threats; and

indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination comprises indicting, in a portion of the plurality of different portions that corresponds to the particular network threat, whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

16. The method of claim 11, comprising:

determining, by the packet-filtering device, an ordering of the plurality of network threats; and

indicating, in the interface, the ordering.

17. The method of claim 16, wherein determining the ordering comprises determining the ordering based on data stored in a packet-flow log, the method comprising, for each packet of the plurality of packets and responsive to the determination by the packet-filtering device that the packet corresponds to the one or more criteria that correspond to the one or more network-threat indicators, updating, by the packet-filtering device and based on the packet-log entry, the packet-flow log to indicate the determination and whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

18. The method of claim 17, wherein determining the ordering comprises, for each network threat of the plurality of network threats, determining a number of packets corresponding to the network threat and allowed by the packet-filtering device to continue toward their respective destinations.

19. The method of claim 17, wherein determining the ordering comprises, for each network threat of the plurality of network threats, determining a number of packets corresponding to the network threat and prevented by the packet-filtering device from continuing toward their respective destinations.

20. The method of claim 17, wherein determining the ordering comprises, for each network threat of the plurality of network threats, determining a time indicated by the data stored in the packet-flow log at which the packet-filtering device last identified a packet corresponding to the network threat.

21. The method of claim 11, wherein receiving the plurality of packet-filtering rules comprises receiving a plurality of packet-filtering rules generated based on a plurality of network-threat-intelligence reports produced by one or more network-threat-intelligence providers.

22. The method of claim 21, comprising:

    determining, by the packet-filtering device and based on the plurality of network-threat-intelligence reports, an ordering of the plurality of network threats; and

    indicating, in the interface, the ordering.

23. The method of claim 22, wherein:

    a first network threat of the plurality of network threats corresponds to a first packet-filtering rule of the plurality of packet-filtering rules;

    a second network threat of the plurality of network threats corresponds to a second packet-filtering rule of the plurality of packet-filtering rules; and

    determining the ordering comprises determining an order of the first network threat relevant to the second network threat based on:

    a determination that the first packet-filtering rule was generated based on one or more network-threat indicators included in a network-threat-intelligence report of the plurality of network-threat-intelligence reports produced by a first network-threat-intelligence provider of the one or more network-threat-intelligence providers; and

    a determination that the second packet-filtering rule was generated based on one or more network-threat indicators included in a network-threat-intelligence report of the plurality of network-threat-intelligence reports produced by a second network-threat-intelligence provider of the one or more network-threat-intelligence providers.

24. The method of claim 22, wherein:

    a first network threat of the plurality of network threats corresponds to a first packet-filtering rule of the plurality of packet-filtering rules;

    a second network threat of the plurality of network threats corresponds to a second packet-filtering rule of the plurality of packet-filtering rules;

    the first packet-filtering rule was generated based on one or more network-threat indicators included in a first portion of the plurality of network-threat-intelligence reports;

    the second packet-filtering rule was generated based on one or more network-threat indicators included in a second portion of the plurality of network-threat-intelligence reports; and determining the ordering comprises determining an order of the first network threat relevant to the second network threat based on a determination that the first portion of the plurality of network-threat-intelligence reports was received from a greater number of the one or more network-threat-intelligence providers than the second portion of the plurality of network-threat-intelligence reports.

25. The method of claim 22, wherein:

receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices;

a first network threat of the plurality of network threats corresponds to a first packet-filtering rule of the plurality of packet-filtering rules;

a second network threat of the plurality of network threats corresponds to a second packet-filtering rule of the plurality of packet-filtering rules; and

determining the ordering comprises determining an order of the first network threat relevant to the second network threat based on data received from the one or more computing devices indicating a number of the plurality of different packet-filtering devices that have reconfigured an operator of the first packet-filtering rule to prevent packets corresponding to criteria specified by the first packet-filtering rule from continuing toward their respective destinations.

26. The method of claim 1, wherein the plurality of packets comprises a first portion of packets and a second portion of packets, each packet in the first portion of packets corresponding to one or more particular criteria, specified by a particular packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more particular network-threat indicators of the plurality of network-threat indicators, and each packet in the second portion of packets corresponding to the one or more particular criteria, the method comprising:

applying, by the packet-filtering device and to each packet in the first portion of packets, an operator specified by the particular packet-filtering rule and configured to cause the packet-filtering device to allow the packet to continue toward its destination;

allowing, by the packet-filtering device, each packet in the first portion of packets to continue toward its destination; and after allowing each packet in the first portion of packets to continue toward its destination:

reconfiguring the operator specified by the particular packet-filtering rule to cause the packet-filtering device to prevent packets corresponding to the one or more particular criteria from continuing toward their respective destinations;

applying, by the packet-filtering device and to each packet in the second portion of packets, the operator specified by the particular packet-filtering rule; and

preventing, by the packet-filtering device, each packet in the second portion of packets from continuing toward its destination.

27. The method of claim 26, wherein reconfiguring the operator comprises reconfiguring the operator in response to receiving an instruction from the user device.

28. The method of claim 27, wherein:

each of the plurality of network-threat indicators corresponds to at least one network threat of a plurality of network threats;

each of the plurality of packet-filtering rules corresponds to a different network threat of the plurality of network threats;

the particular packet-filtering rule corresponds to a particular network threat of the plurality of network threats;

the interface comprises a plurality of different portions;

each portion of the plurality of different portions corresponds to a different packet-filtering rule of the plurality of packet-filtering rules and a different network threat of the plurality of network threats; and

receiving the instruction comprises receiving an instruction generated by the user device in response to a user invoking an element of the interface located in a portion of the plurality of portions corresponding to the particular packet-filtering rule and the particular network threat.

29. The method of claim 26, wherein the packet-filtering device is located at a boundary between a first network and a second network, each packet in the first portion of packets and each packet in the second portion of packets is either received from a common host in the first network and destined for a common host in the second network or received from the common host in the second network and destined for the common host in the first network, the method comprising:

generating, by the packet-filtering device, one or more packet-filtering rules configured to cause the packet-filtering device to prevent packets received from the common host in the first network from continuing toward at least one of one or more other hosts in the first network or one or more other hosts in the second network; and

responsive to an instruction received from the user device:

applying, by the packet-filtering device, the one or more packet-filtering rules to one or more packets received from the common host in the first network; and

preventing, by the packet-filtering device, the one or more packets received from the common host in the first network from continuing toward the at least one of the one or more other hosts in the first network or the one or more other hosts in the second network.

30. The method of claim 26, wherein:

receiving the plurality of packet-filtering rules comprises receiving the plurality of packet-filtering rules from one or more computing devices that provide packet-filtering rules to a plurality of different packet-filtering devices; and

reconfiguring the operator comprises reconfiguring the operator in response to receiving data from the one or more computing devices.

31. A packet-filtering device comprising:

at least one processor; and

a memory storing instructions that when executed by the at least one processor cause the packet-filtering device to:

receive a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;

receive a plurality of packets; and

for each packet of the plurality of packets and responsive to a determination that the packet corresponds to one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators:

apply, to the packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to either prevent the packet from continuing toward its destination or allow the packet to continue toward its destination;

generate a packet-log entry comprising information from the packet-filtering rule that identifies the one or more network-threat indicators and indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination;

generate, based on the packet-log entry, data indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination;

communicate, to a user device, the data; and

indicate, based on the data, in an interface displayed by the user device, and in a portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators, whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

32. One or more non-transitory computer-readable media comprising instructions that when executed by at least one processor of a packet-filtering device cause the packet-filtering device to:

receive a plurality of packet-filtering rules configured to cause the packet-filtering device to identify packets corresponding to at least one of a plurality of network-threat indicators;

receive a plurality of packets; and

for each packet of the plurality of packets and responsive to a determination that the packet corresponds to one or more criteria, specified by a packet-filtering rule of the plurality of packet-filtering rules, that correspond to one or more network-threat indicators of the plurality of network-threat indicators:

apply, to the packet, an operator specified by the packet-filtering rule and configured to cause the packet-filtering device to either prevent the packet from continuing toward its destination or allow the packet to continue toward its destination;

generate a packet-log entry comprising information from the packet-filtering rule that identifies the one or more network-threat indicators and indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination;

generate, based on the packet-log entry, data indicating whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination;

communicate, to a user device, the data; and

indicate, based on the data, in an interface displayed by the user device, and in a portion of the interface corresponding to the packet-filtering rule and the one or more network-threat indicators, whether the packet-filtering device prevented the packet from continuing toward its destination or allowed the packet to continue toward its destination.

33. The method of claim 1, wherein applying the operator comprises applying an operator determined based on one or more scores associated with the one or more network-threat indicators.

34. The method of claim 33, comprising determining the one or more scores based on data received from one or more network-threat-intelligence providers.

35. The method of claim 34, wherein determining the one or more scores comprises:

determining a network-threat-intelligence provider of the one or more network-threat-intelligence providers from which a network-threat indicator of the one or more network-threat indicators was received; and

determining a score for the network-threat indicator based on the network-threat-intelligence provider.

36. The method of claim 34, wherein determining the one or more scores comprises:

determining a number of network-threat-intelligence providers of the one or more network-threat-intelligence providers from which a network-threat indicator of the one or more network-threat indicators was received; and

determining a score for the network-threat indicator based on the number of network-threat-intelligence providers.

37. The method of claim 33, comprising determining the one or more scores based on a number of the plurality of packets that correspond to the one or more criteria.

38. The method of claim 33, comprising determining the one or more scores based on one or more times at which one or more packets of the plurality of packets that correspond to the one or more criteria were received by the packet-filtering device.

39. The method of claim 33, comprising determining the one or more scores based on a time at which a packet of the plurality of packets that corresponds to the one or more criteria was last received by the packet-filtering device.

40. The method of claim 33, comprising determining the one or more scores based on a destination of a packet of the plurality of packets that corresponds to the one or more criteria.

41. The method of claim 33, comprising determining the one or more scores based on at least one of a type of threat associated with a network-threat indicator of the one or more network-threat indicators, geographic information associated with a network-threat indicator of the one or more network-threat indicators, an anonymous proxy associated with a network-threat indicator of the one or more network-threat indicators, or an actor associated with a network-threat indicator of the one or more network-threat indicators.

42. The method of claim 33, comprising indicating, in the interface displayed by the user device, the one or more scores.

43. The method of claim 33, comprising indicating, in the interface displayed by the user device, an ordering of the plurality of packet-filtering rules determined based on the one or more scores.

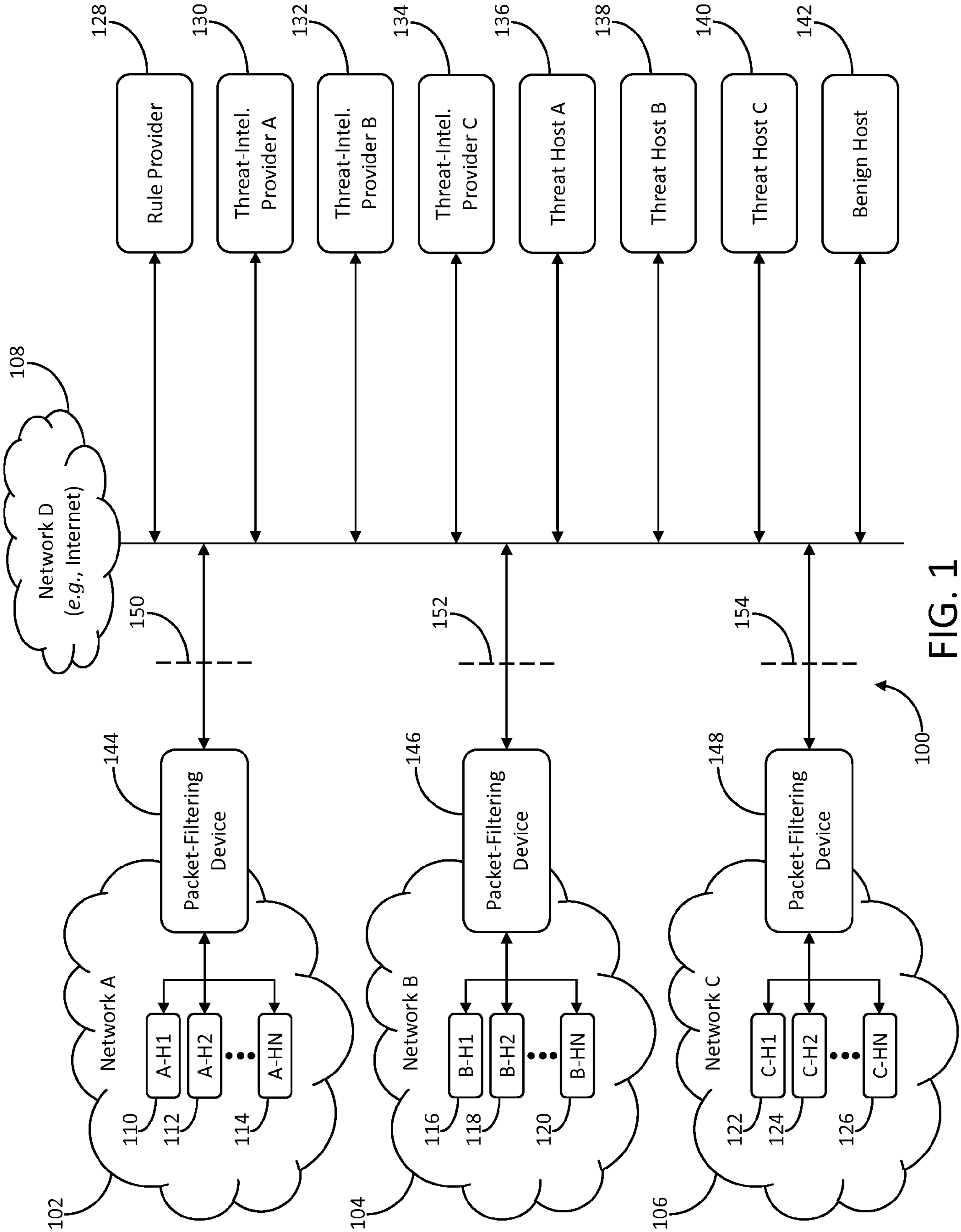

Network D
(*e.g.*, Internet)
108
Rule Provider
128
Threat-Intel. Provider A
130
Threat-Intel. Provider B
132
Threat-Intel. Provider C
134
Threat Host A
136
Threat Host B
138
Threat Host C
140
Benign Host
142
150
152
154
Packet-Filtering Device
144
Packet-Filtering Device
146
Packet-Filtering Device
148
Network A
102
A-H1
A-H2
A-HN
110
112
114
Network B
104
B-H1
B-H2
B-HN
116
118
120
Network C
106
C-H1
C-H2
C-HN
122
124
126
100

FIG. 1

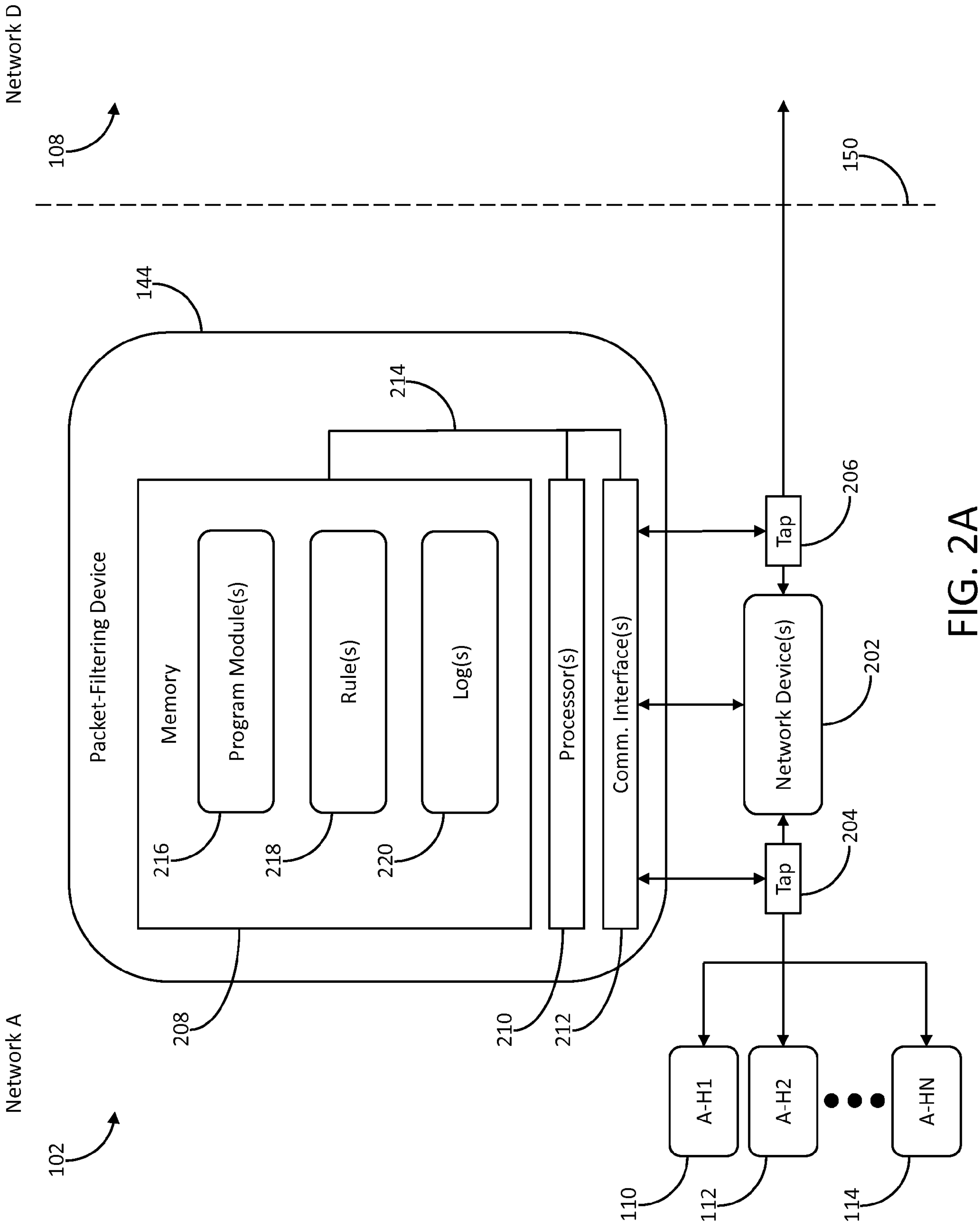

Network D
108
Network A
102
144
Packet-Filtering Device
Memory
Program Module(s)
Rule(s)
Log(s)
Processor(s)
Comm. Interface(s)
214
216
218
220
208
210
212
Tap
206
Tap
204
Network Device(s)
202
150
A-H1
A-H2
A-HN
110
112
114

FIG. 2A

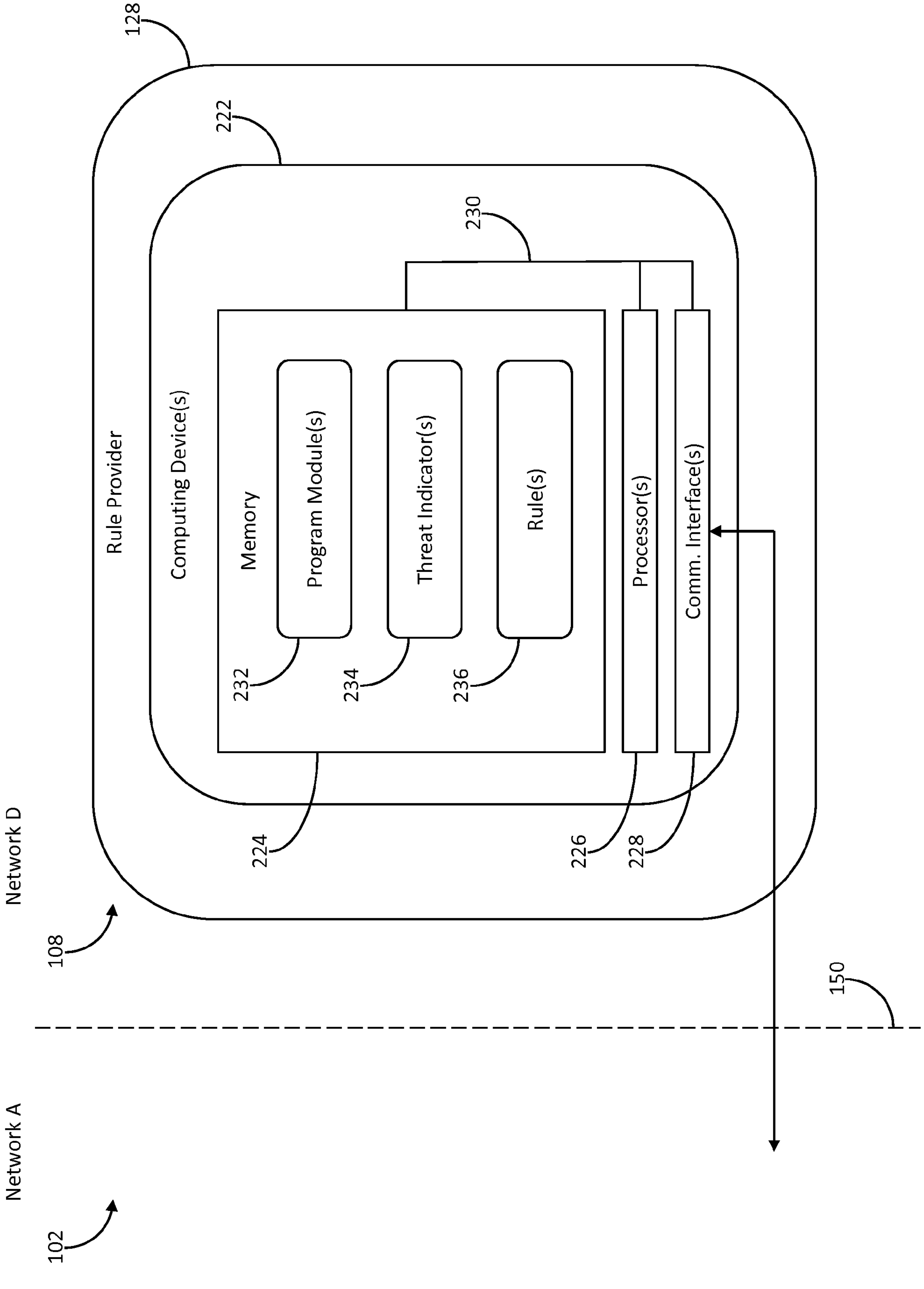

128
Rule Provider
222
Computing Device(s)
230
Memory
Program Module(s)
Threat Indicator(s)
Rule(s)
Processor(s)
Comm. Interface(s)
232
234
236
224
226
228
Network D
108
150
Network A
102

FIG. 2B

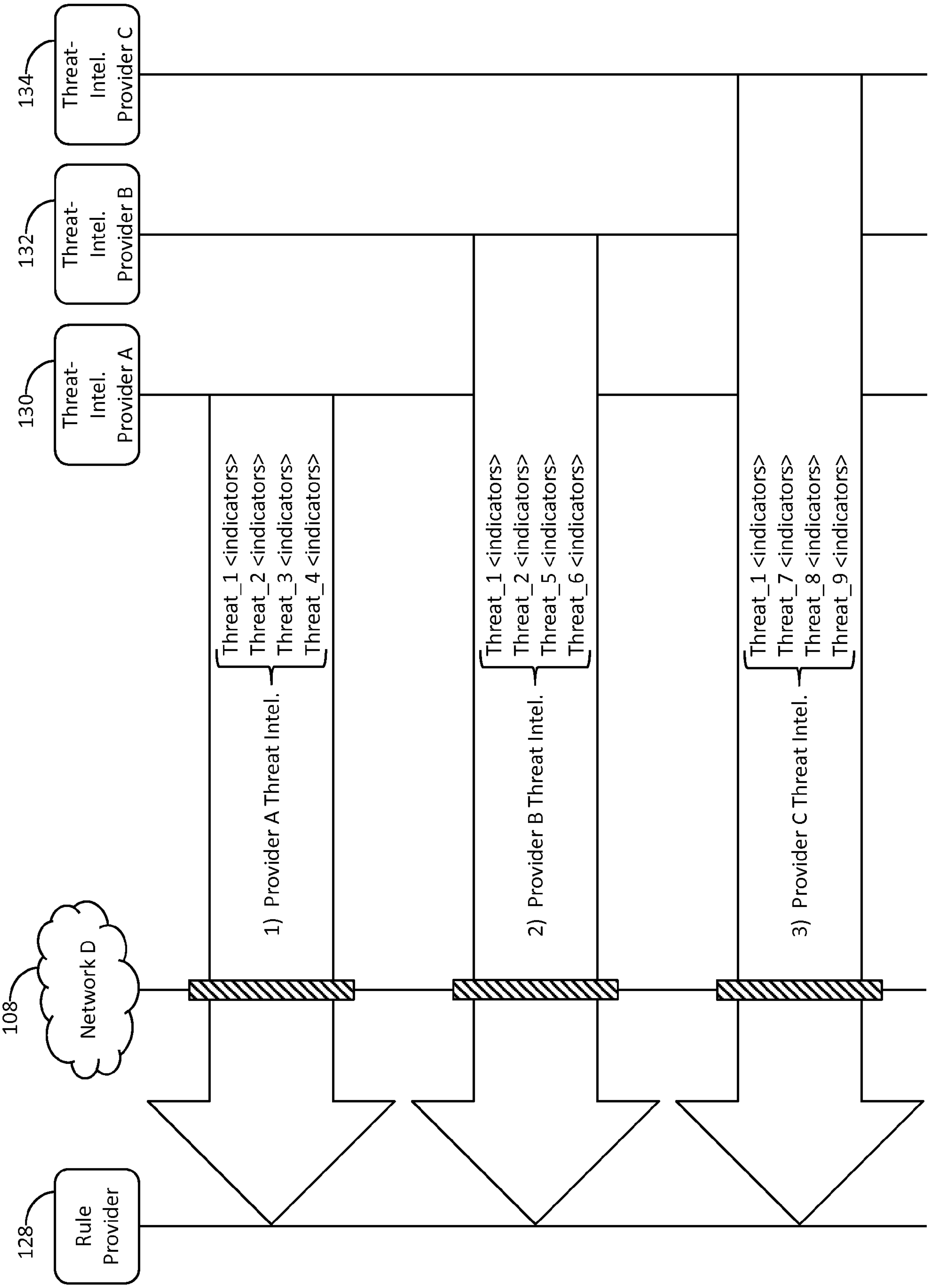

134
Threat-Intel. Provider C
132
Threat-Intel. Provider B
130
Threat-Intel. Provider A
108
Network D
128
Rule Provider
1) Provider A Threat Intel.
Threat_1 <indicators>
Threat_2 <indicators>
Threat_3 <indicators>
Threat_4 <indicators>
2) Provider B Threat Intel.
Threat_1 <indicators>
Threat_2 <indicators>
Threat_5 <indicators>
Threat_6 <indicators>
3) Provider C Threat Intel.
Threat_1 <indicators>
Threat_7 <indicators>
Threat_8 <indicators>
Threat_9 <indicators>

FIG. 3A

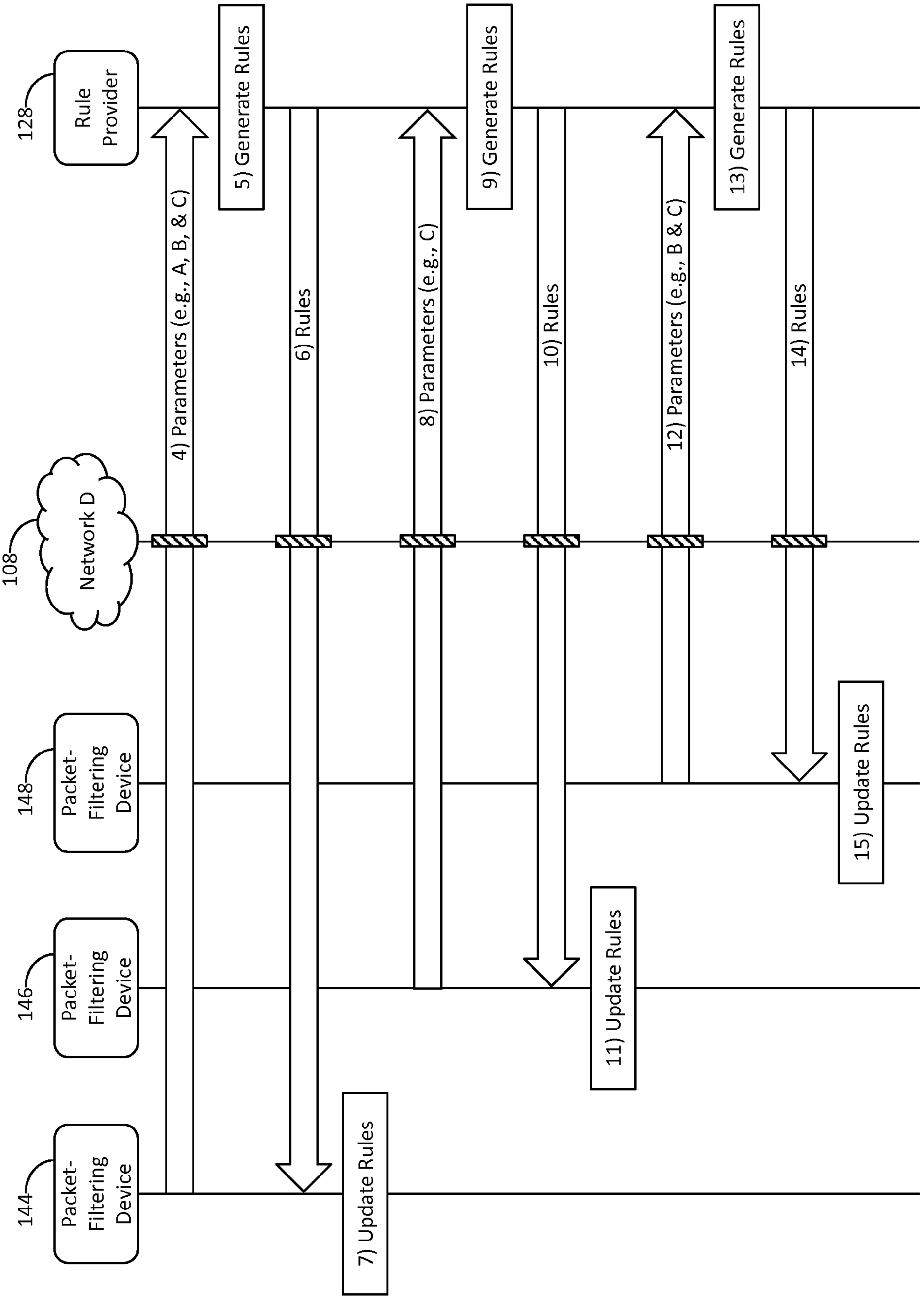

128
Rule Provider
108
Network D
148
Packet-Filtering Device
146
Packet-Filtering Device
144
Packet-Filtering Device
4) Parameters (e.g., A, B, & C)
5) Generate Rules
6) Rules
7) Update Rules
8) Parameters (e.g., C)
9) Generate Rules
10) Rules
11) Update Rules
12) Parameters (e.g., B & C)
13) Generate Rules
14) Rules
15) Update Rules

FIG. 3B

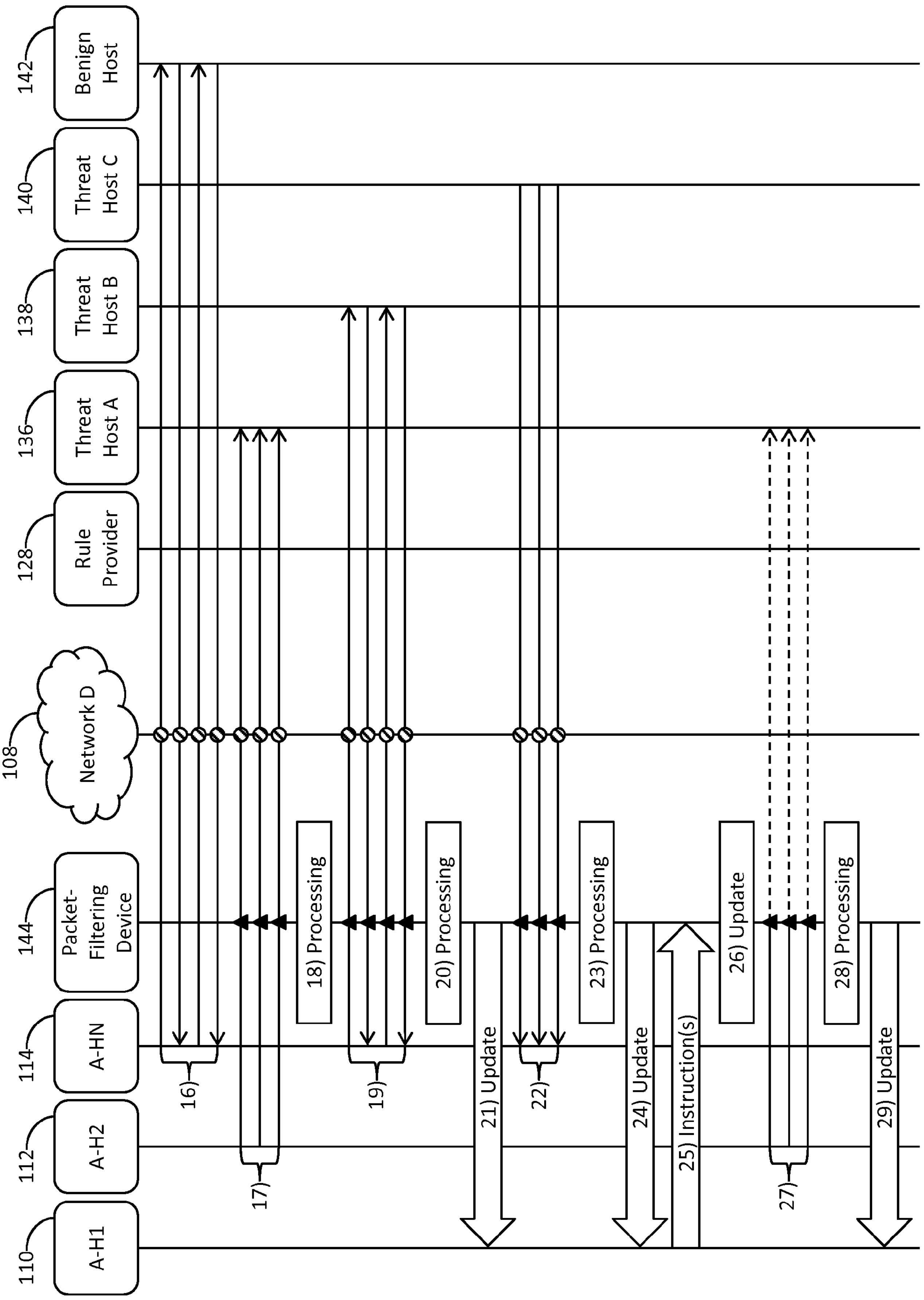

142
Benign Host
140
Threat Host C
138
Threat Host B
136
Threat Host A
128
Rule Provider
108
Network D
144
Packet-Filtering Device
114
A-HN
112
A-H2
110
A-H1
16)
17)
18) Processing
19)
20) Processing
21) Update
22)
23) Processing
24) Update
25) Instruction(s)
26) Update
27)
28) Processing
29) Update

FIG. 3C

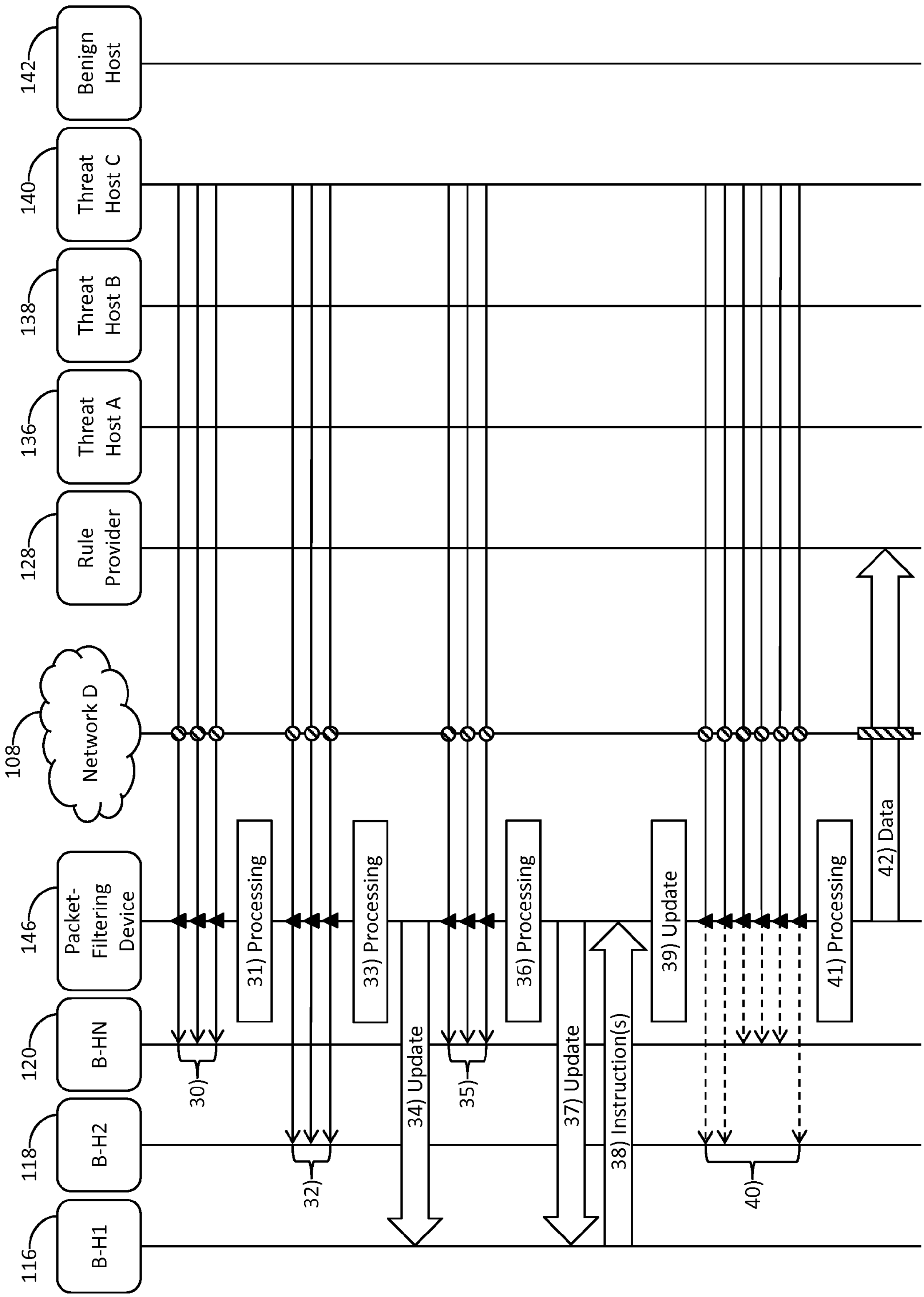

142
Benign Host
140
Threat Host C
138
Threat Host B
136
Threat Host A
128
Rule Provider
108
Network D
146
Packet-Filtering Device
120
B-HN
118
B-H2
116
B-H1
30)
31) Processing
32)
33) Processing
34) Update
35)
36) Processing
37) Update
38) Instruction(s)
39) Update
40)
41) Processing
42) Data

FIG. 3D

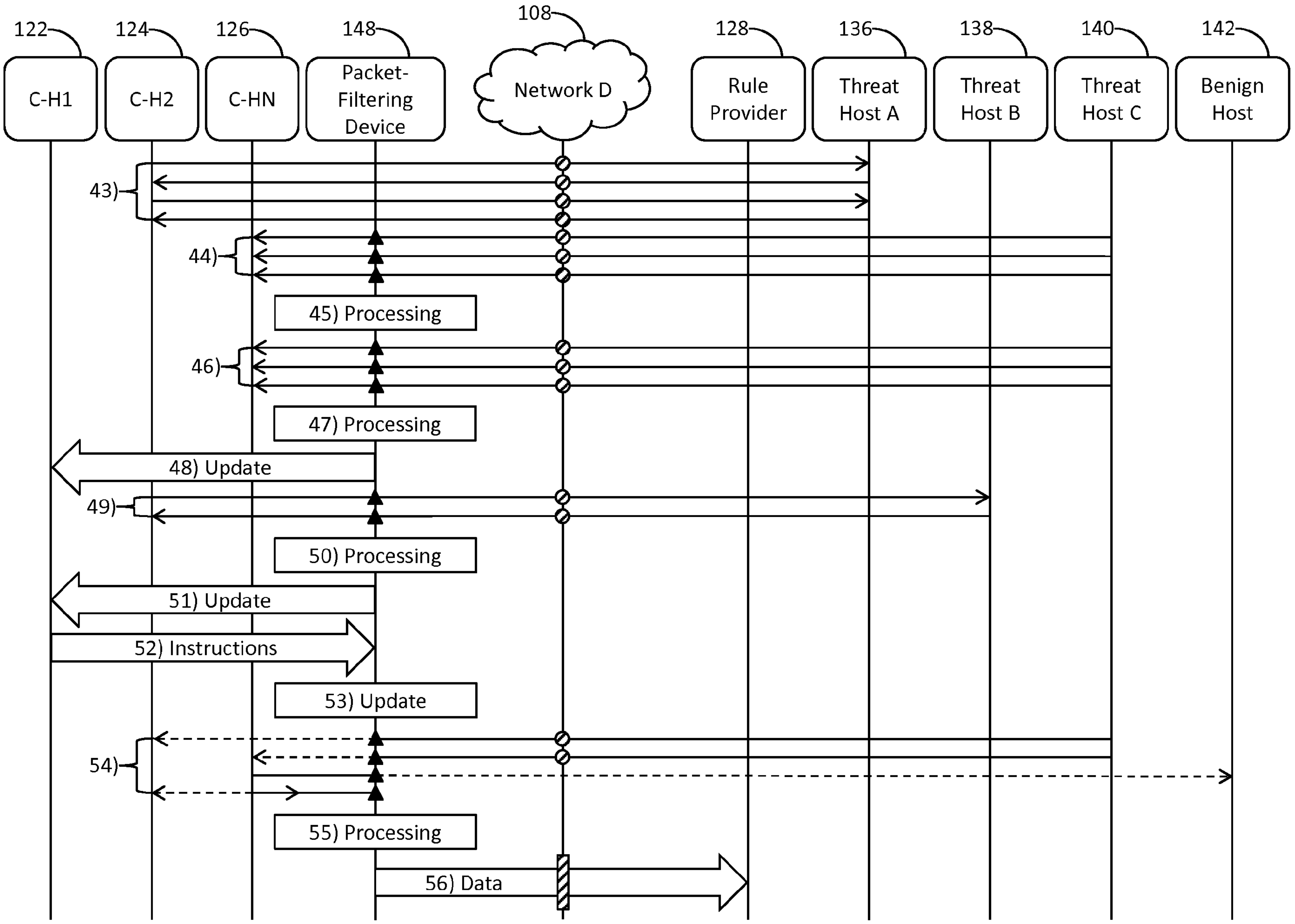

122
124
126
148
108
128
136
138
140
142
C-H1
C-H2
C-HN
Packet-
Filtering
Device
Network D
Rule
Provider
Threat
Host A
Threat
Host B
Threat
Host C
Benign
Host
43)
44)
45) Processing
46)
47) Processing
48) Update
49)
50) Processing
51) Update
52) Instructions
53) Update
54)
55) Processing
56) Data

FIG. 3E

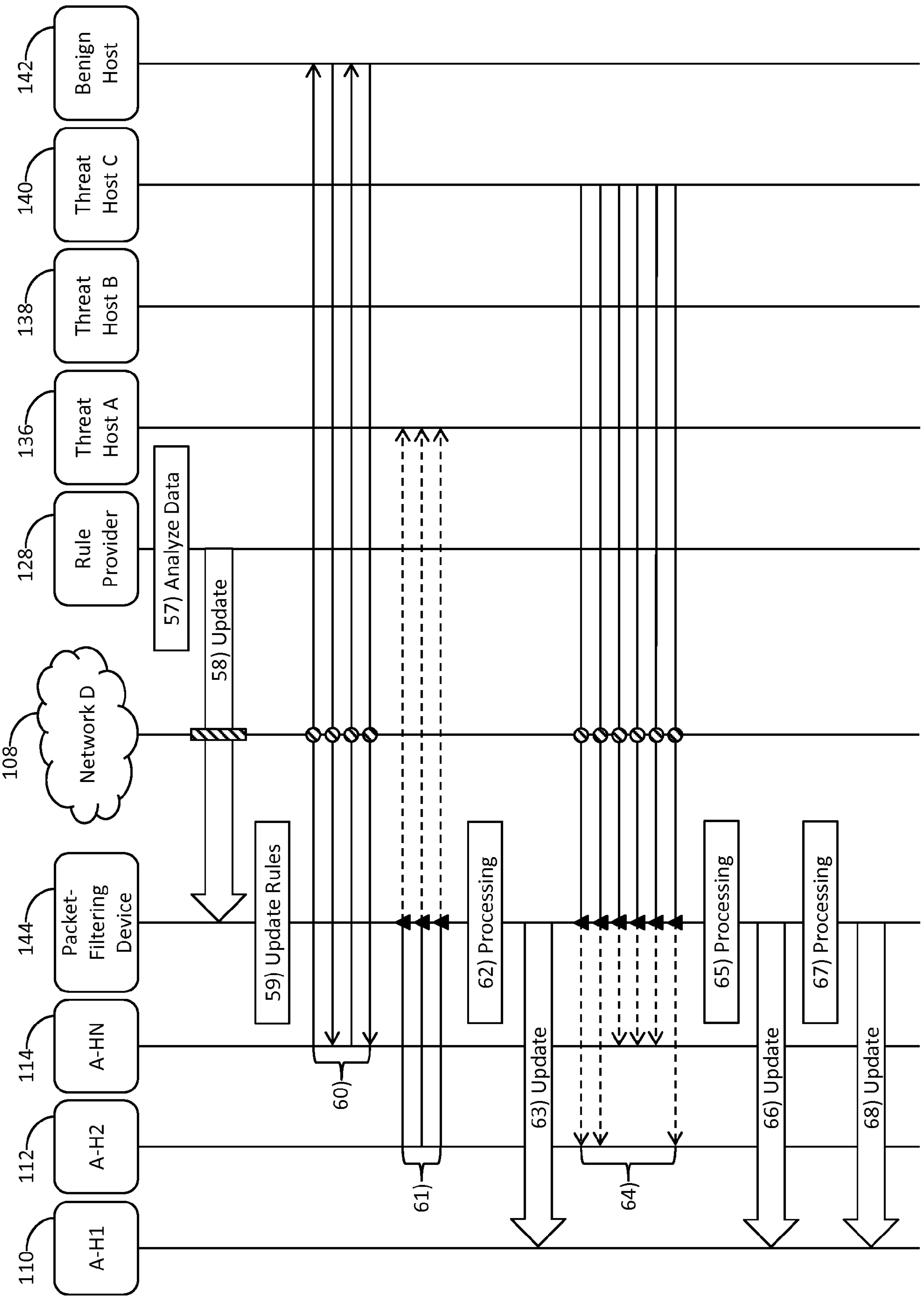
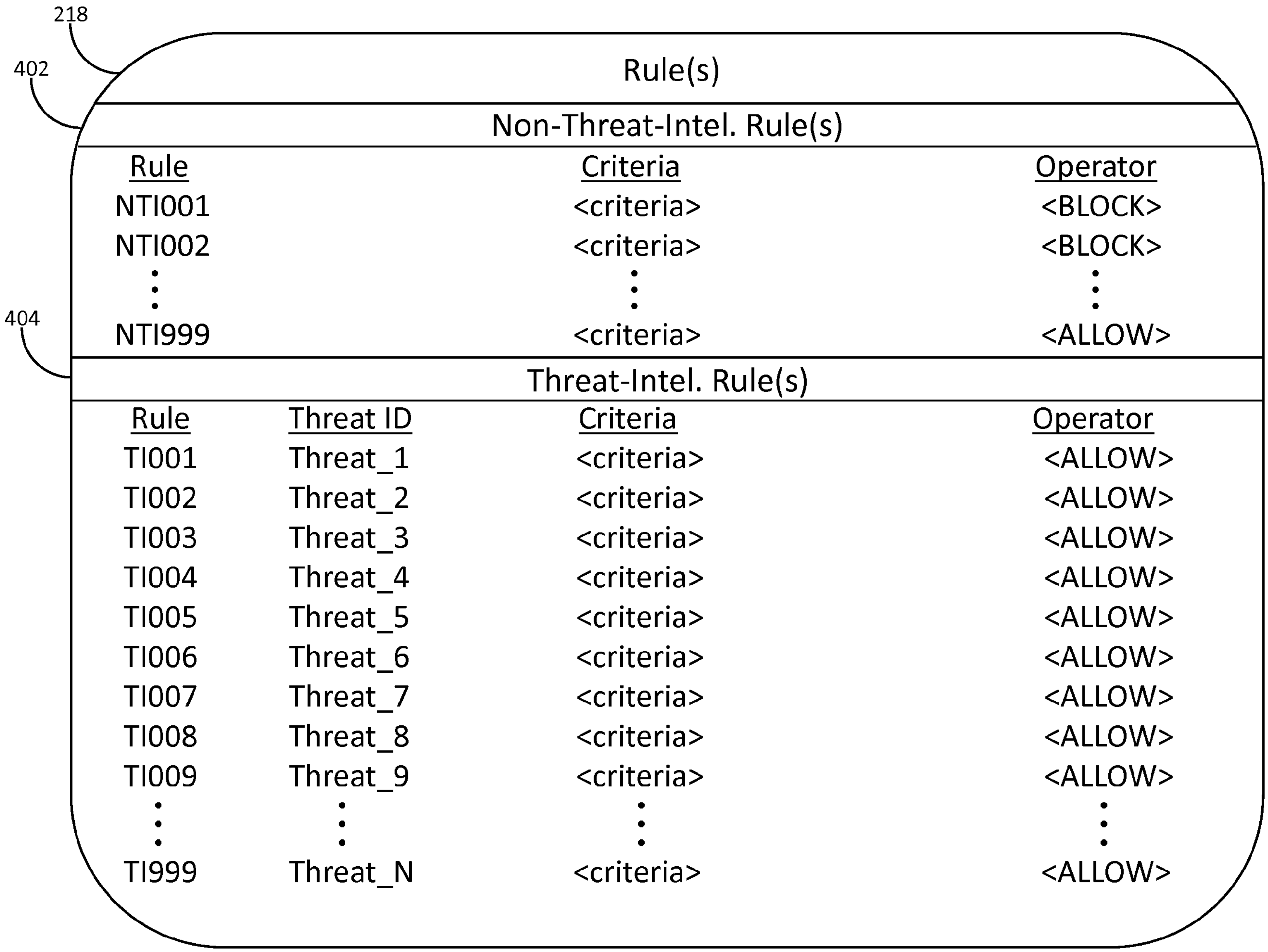

142
Benign Host
140
Threat Host C
138
Threat Host B
136
Threat Host A
128
Rule Provider
108
Network D
144
Packet-Filtering Device
114
A-HN
112
A-H2
110
A-H1
57) Analyze Data
58) Update
59) Update Rules
60)
61)
62) Processing
63) Update
64)
65) Processing
66) Update
67) Processing
68) Update

FIG. 3F



Rule(s)

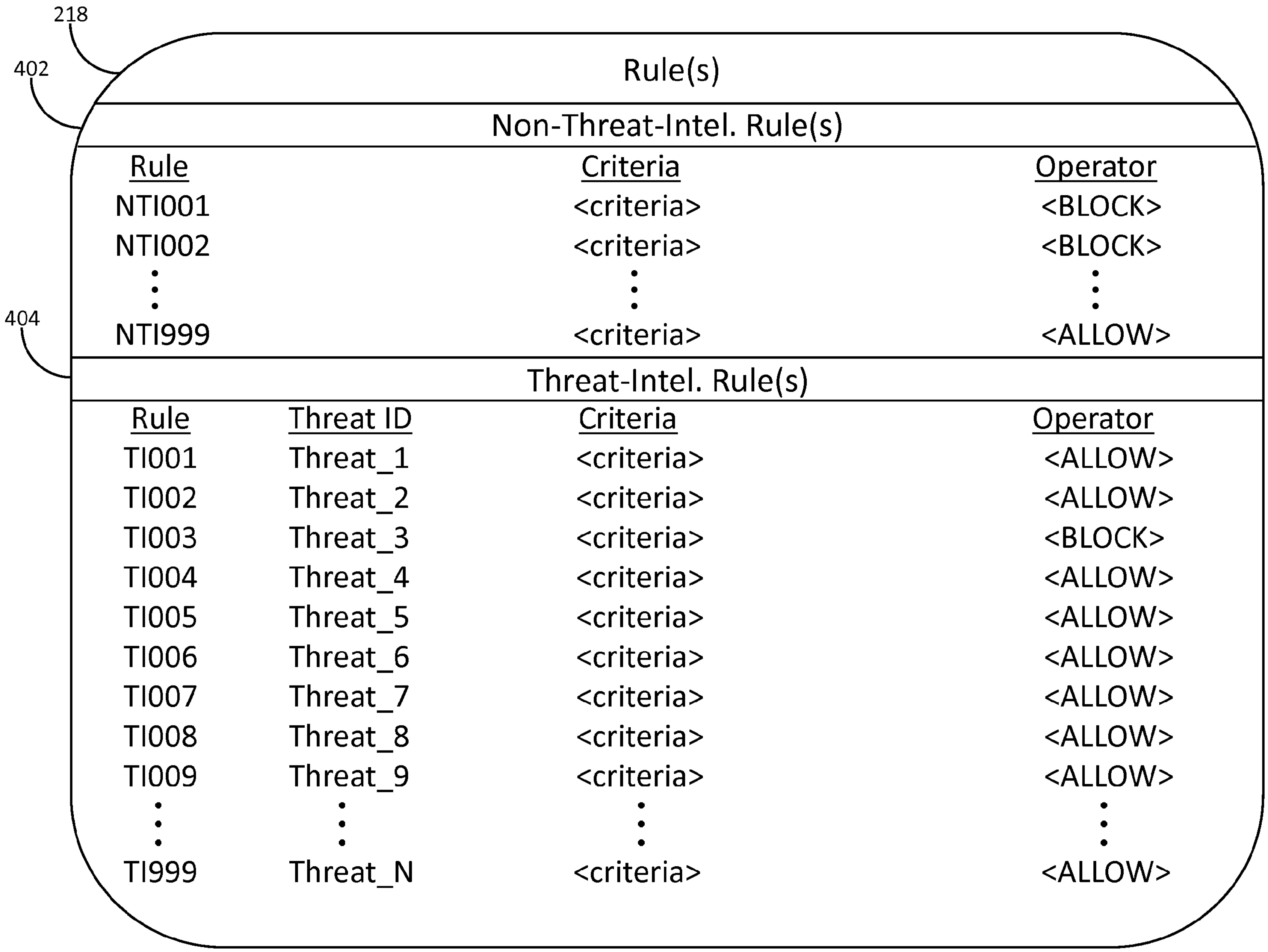
Non-Threat-Intel. Rule(s)

Rule	Criteria	Operator
NTI001	<criteria>	<BLOCK>
NTI002	<criteria>	<BLOCK>
⋮	⋮	⋮
NTI999	<criteria>	<ALLOW>

Threat-Intel. Rule(s)

Rule	Threat ID	Criteria	Operator
TI001	Threat_1	<criteria>	<ALLOW>
TI002	Threat_2	<criteria>	<ALLOW>
TI003	Threat_3	<criteria>	<ALLOW>
TI004	Threat_4	<criteria>	<ALLOW>
TI005	Threat_5	<criteria>	<ALLOW>
TI006	Threat_6	<criteria>	<ALLOW>
TI007	Threat_7	<criteria>	<ALLOW>
TI008	Threat_8	<criteria>	<ALLOW>
TI009	Threat_9	<criteria>	<ALLOW>
⋮	⋮	⋮	⋮
TI999	Threat_N	<criteria>	<ALLOW>

FIG. 4A



Rule(s)

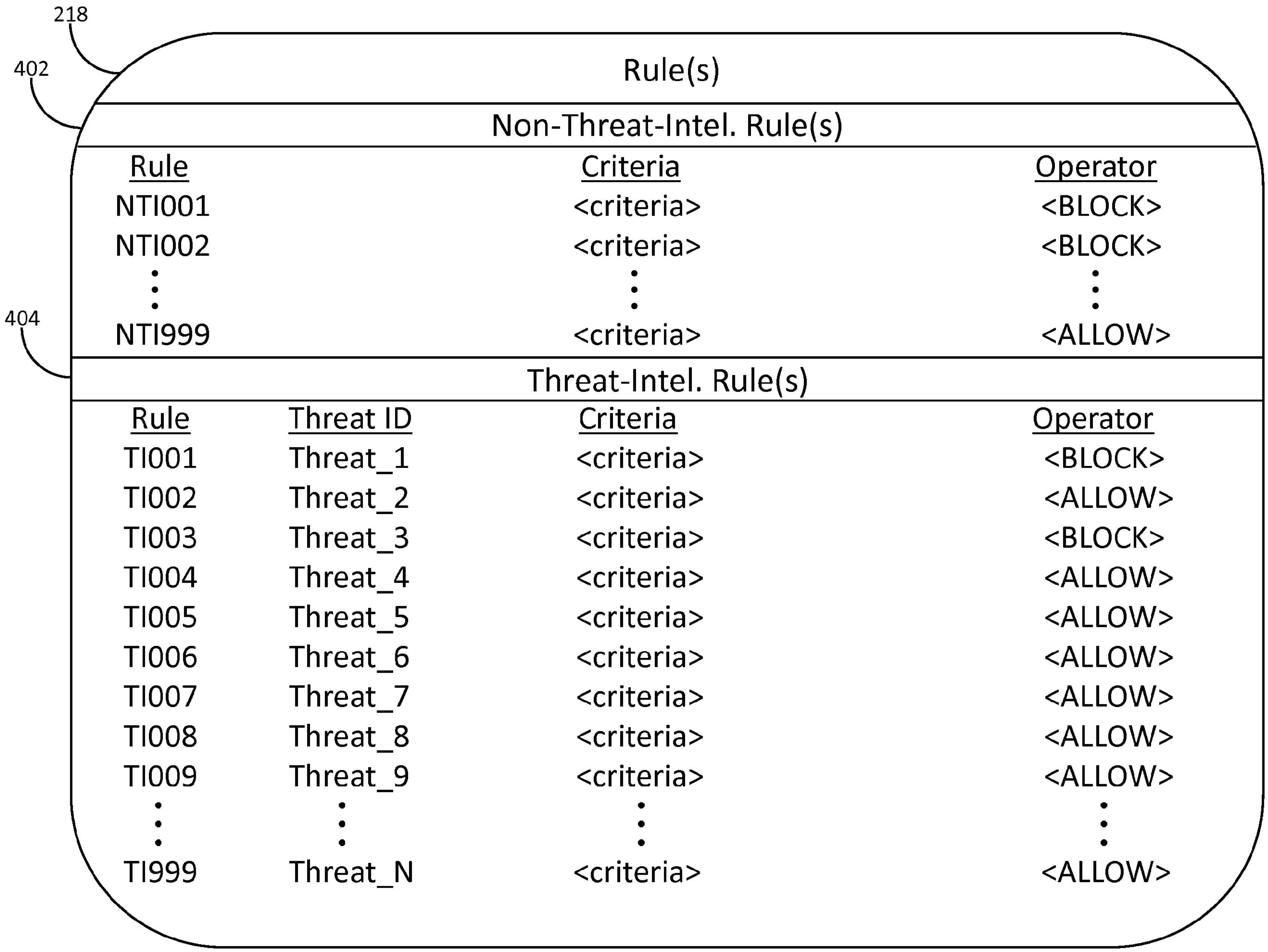
Non-Threat-Intel. Rule(s)

Rule	Criteria	Operator
NTI001	<criteria>	<BLOCK>
NTI002	<criteria>	<BLOCK>
⋮	⋮	⋮
NTI999	<criteria>	<ALLOW>

Threat-Intel. Rule(s)

Rule	Threat ID	Criteria	Operator
TI001	Threat_1	<criteria>	<ALLOW>
TI002	Threat_2	<criteria>	<ALLOW>
TI003	Threat_3	<criteria>	<BLOCK>
TI004	Threat_4	<criteria>	<ALLOW>
TI005	Threat_5	<criteria>	<ALLOW>
TI006	Threat_6	<criteria>	<ALLOW>
TI007	Threat_7	<criteria>	<ALLOW>
TI008	Threat_8	<criteria>	<ALLOW>
TI009	Threat_9	<criteria>	<ALLOW>
⋮	⋮	⋮	⋮
TI999	Threat_N	<criteria>	<ALLOW>

FIG. 4B



Rule(s)

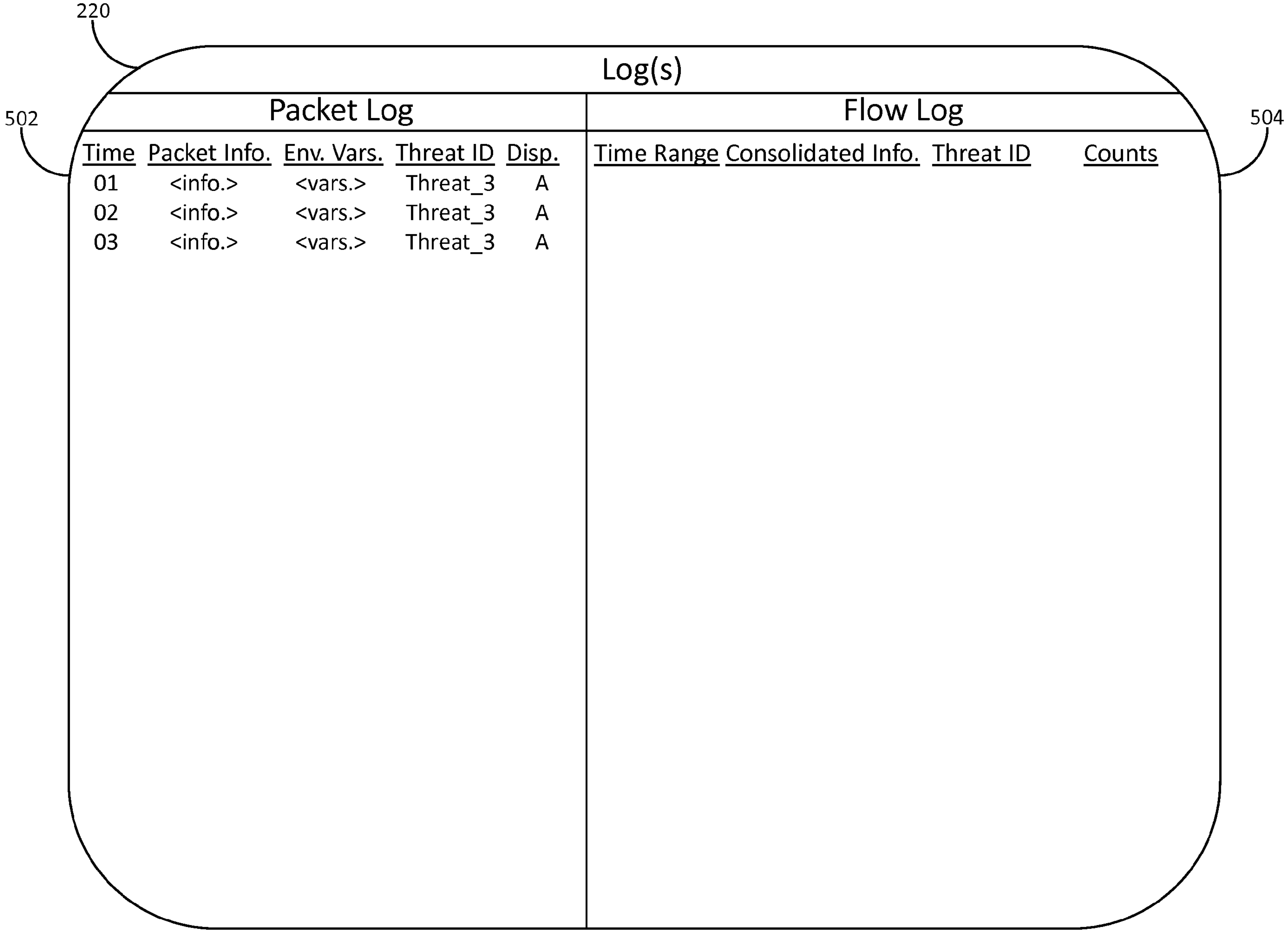
Non-Threat-Intel. Rule(s)

Rule	Criteria	Operator
NTI001	<criteria>	<BLOCK>
NTI002	<criteria>	<BLOCK>
⋮	⋮	⋮
NTI999	<criteria>	<ALLOW>

Threat-Intel. Rule(s)

Rule	Threat ID	Criteria	Operator
TI001	Threat_1	<criteria>	<BLOCK>
TI002	Threat_2	<criteria>	<ALLOW>
TI003	Threat_3	<criteria>	<BLOCK>
TI004	Threat_4	<criteria>	<ALLOW>
TI005	Threat_5	<criteria>	<ALLOW>
TI006	Threat_6	<criteria>	<ALLOW>
TI007	Threat_7	<criteria>	<ALLOW>
TI008	Threat_8	<criteria>	<ALLOW>
TI009	Threat_9	<criteria>	<ALLOW>
⋮	⋮	⋮	⋮
TI999	Threat_N	<criteria>	<ALLOW>

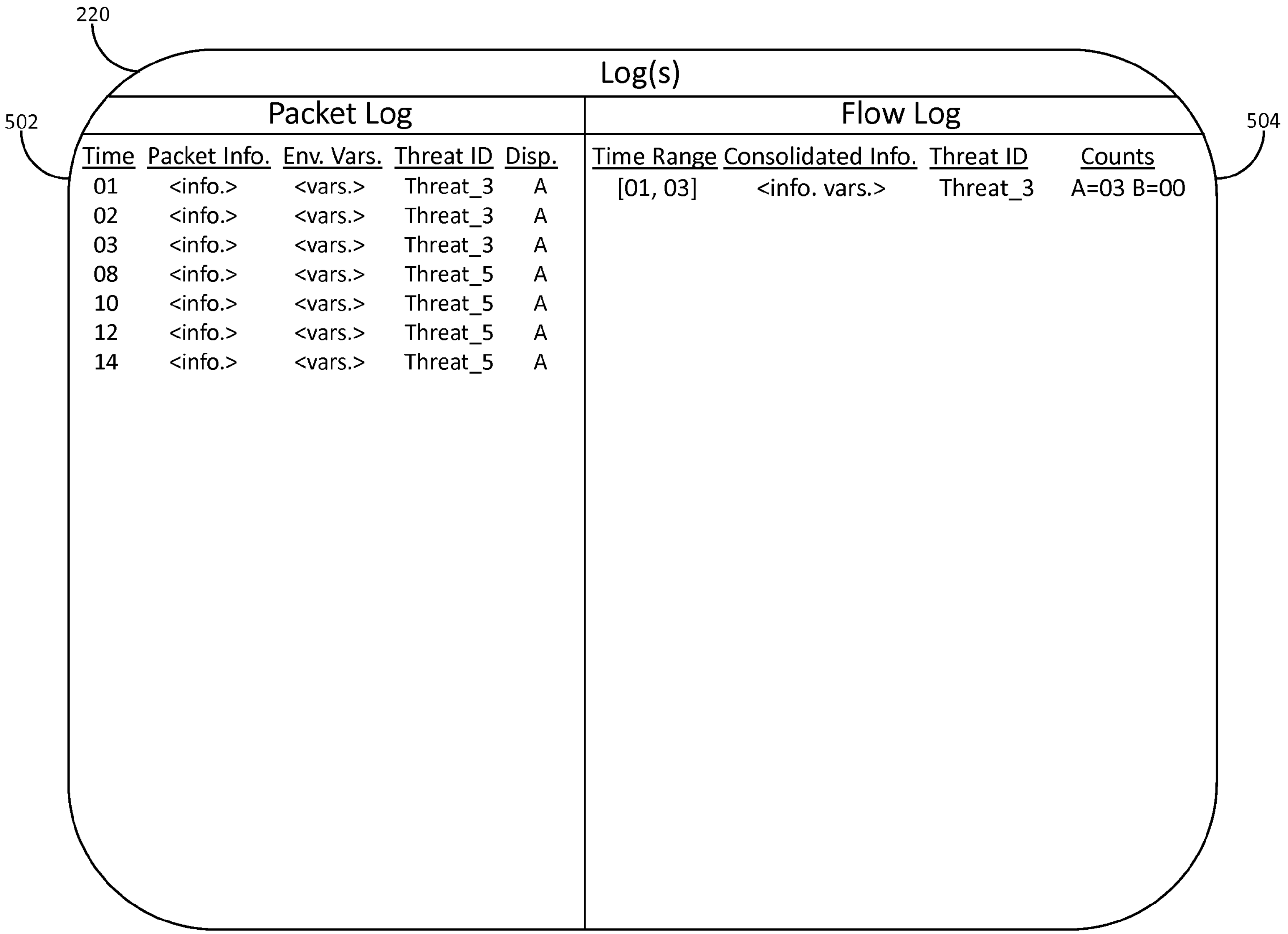
FIG. 4C



Log(s)

Packet Log					Flow Log			
Time	Packet Info.	Env. Vars.	Threat ID	Disp.	Time Range	Consolidated Info.	Threat ID	Counts
01	<info.>	<vars.>	Threat_3	A				
02	<info.>	<vars.>	Threat_3	A				
03	<info.>	<vars.>	Threat_3	A				

FIG. 5A



Log(s)

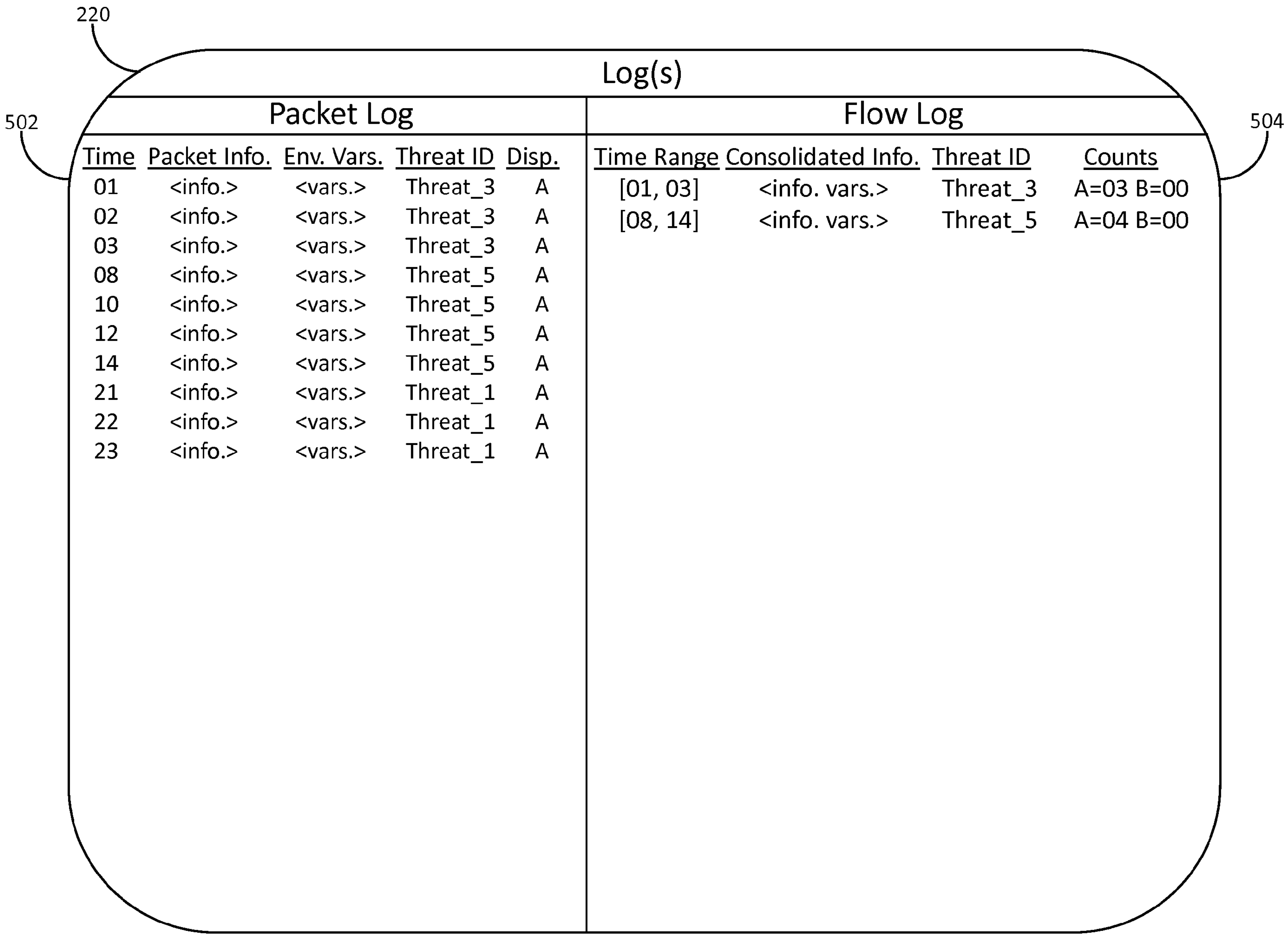
Packet Log

Time	Packet Info.	Env. Vars.	Threat ID	Disp.
01	<info.>	<vars.>	Threat_3	A
02	<info.>	<vars.>	Threat_3	A
03	<info.>	<vars.>	Threat_3	A
08	<info.>	<vars.>	Threat_5	A
10	<info.>	<vars.>	Threat_5	A
12	<info.>	<vars.>	Threat_5	A
14	<info.>	<vars.>	Threat_5	A

Flow Log

Time Range	Consolidated Info.	Threat ID	Counts
[01, 03]	<info. vars.>	Threat_3	A=03 B=00

FIG. 5B



Log(s)

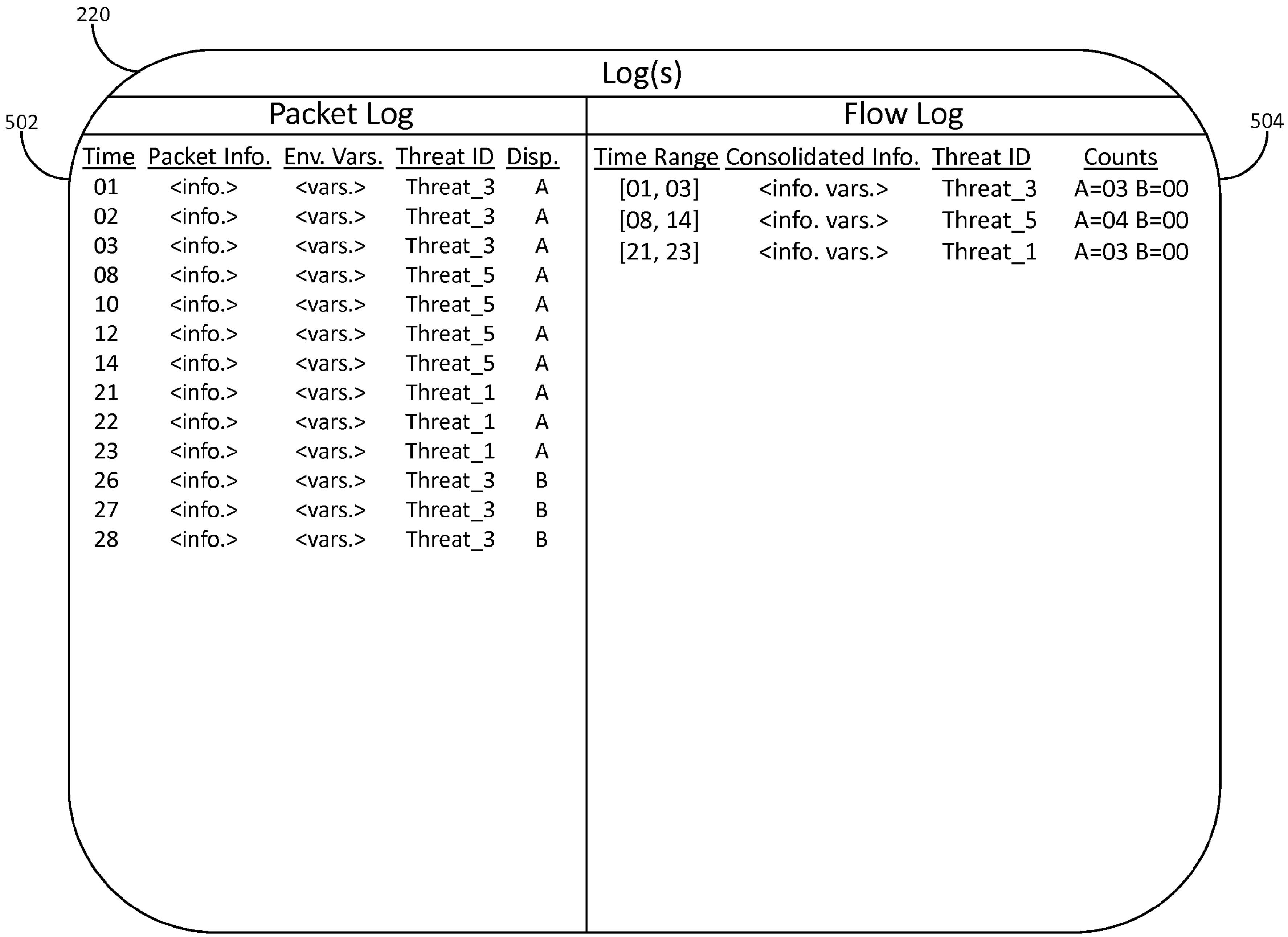
Packet Log

Time	Packet Info.	Env. Vars.	Threat ID	Disp.
01	<info.>	<vars.>	Threat_3	A
02	<info.>	<vars.>	Threat_3	A
03	<info.>	<vars.>	Threat_3	A
08	<info.>	<vars.>	Threat_5	A
10	<info.>	<vars.>	Threat_5	A
12	<info.>	<vars.>	Threat_5	A
14	<info.>	<vars.>	Threat_5	A
21	<info.>	<vars.>	Threat_1	A
22	<info.>	<vars.>	Threat_1	A
23	<info.>	<vars.>	Threat_1	A

Flow Log

Time Range	Consolidated Info.	Threat ID	Counts
[01, 03]	<info. vars.>	Threat_3	A=03 B=00
[08, 14]	<info. vars.>	Threat_5	A=04 B=00

FIG. 5C



Log(s)

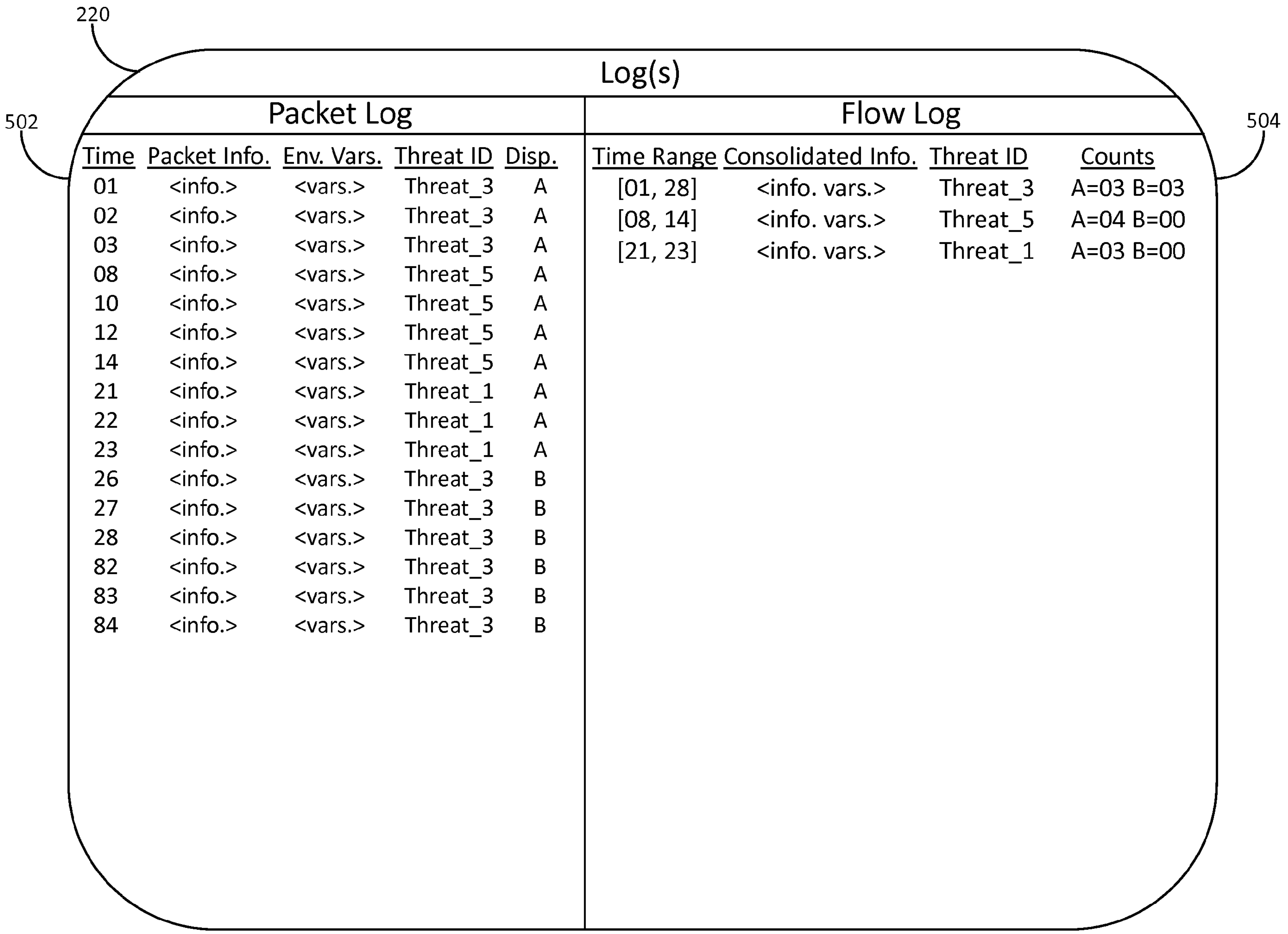
Packet Log

Time	Packet Info.	Env. Vars.	Threat ID	Disp.
01	<info.>	<vars.>	Threat_3	A
02	<info.>	<vars.>	Threat_3	A
03	<info.>	<vars.>	Threat_3	A
08	<info.>	<vars.>	Threat_5	A
10	<info.>	<vars.>	Threat_5	A
12	<info.>	<vars.>	Threat_5	A
14	<info.>	<vars.>	Threat_5	A
21	<info.>	<vars.>	Threat_1	A
22	<info.>	<vars.>	Threat_1	A
23	<info.>	<vars.>	Threat_1	A
26	<info.>	<vars.>	Threat_3	B
27	<info.>	<vars.>	Threat_3	B
28	<info.>	<vars.>	Threat_3	B

Flow Log

Time Range	Consolidated Info.	Threat ID	Counts
[01, 03]	<info. vars.>	Threat_3	A=03 B=00
[08, 14]	<info. vars.>	Threat_5	A=04 B=00
[21, 23]	<info. vars.>	Threat_1	A=03 B=00

FIG. 5D



Log(s)

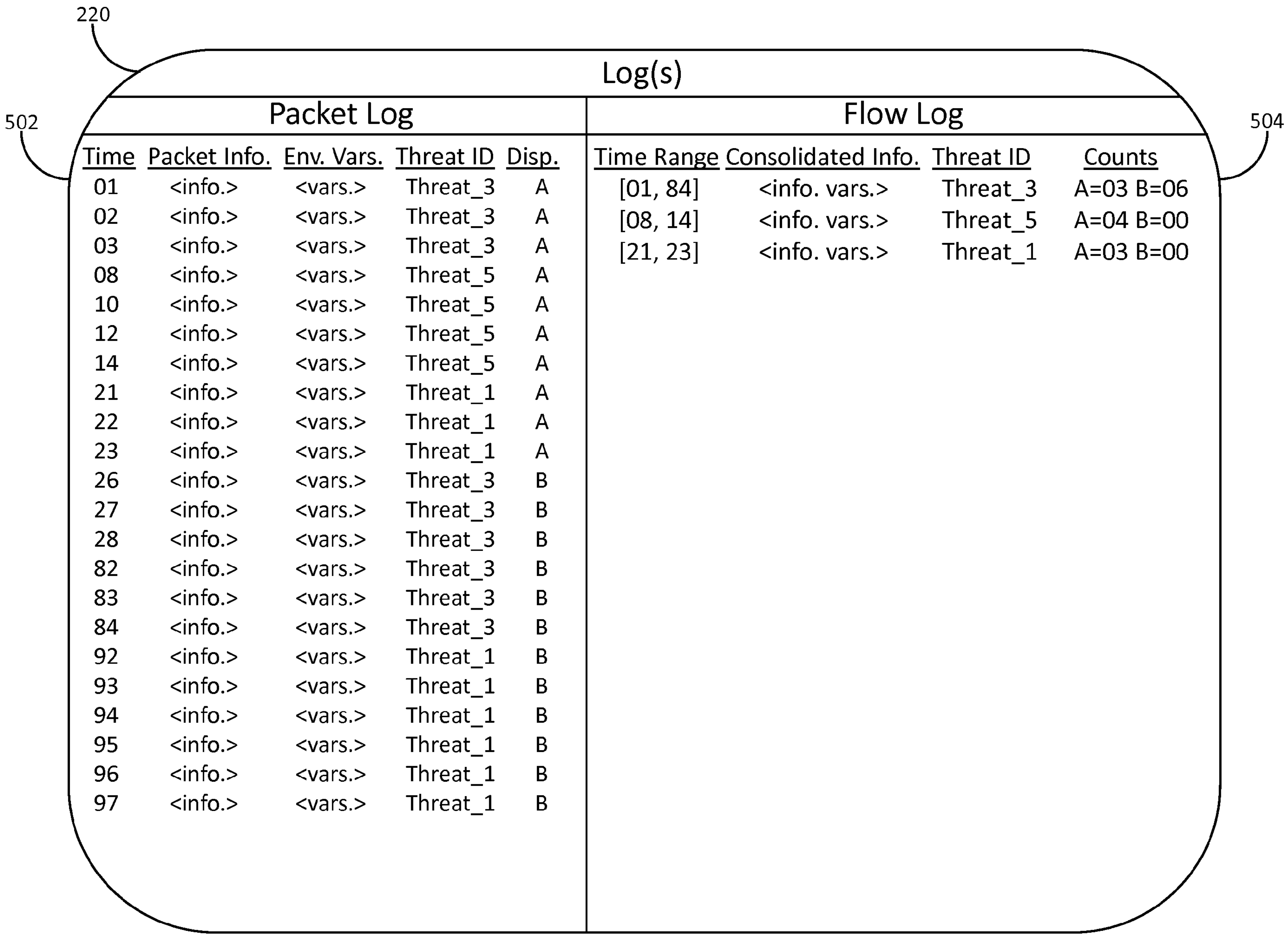
Packet Log

Time	Packet Info.	Env. Vars.	Threat ID	Disp.
01	<info.>	<vars.>	Threat_3	A
02	<info.>	<vars.>	Threat_3	A
03	<info.>	<vars.>	Threat_3	A
08	<info.>	<vars.>	Threat_5	A
10	<info.>	<vars.>	Threat_5	A
12	<info.>	<vars.>	Threat_5	A
14	<info.>	<vars.>	Threat_5	A
21	<info.>	<vars.>	Threat_1	A
22	<info.>	<vars.>	Threat_1	A
23	<info.>	<vars.>	Threat_1	A
26	<info.>	<vars.>	Threat_3	B
27	<info.>	<vars.>	Threat_3	B
28	<info.>	<vars.>	Threat_3	B
82	<info.>	<vars.>	Threat_3	B
83	<info.>	<vars.>	Threat_3	B
84	<info.>	<vars.>	Threat_3	B

Flow Log

Time Range	Consolidated Info.	Threat ID	Counts
[01, 28]	<info. vars.>	Threat_3	A=03 B=03
[08, 14]	<info. vars.>	Threat_5	A=04 B=00
[21, 23]	<info. vars.>	Threat_1	A=03 B=00

FIG. 5E



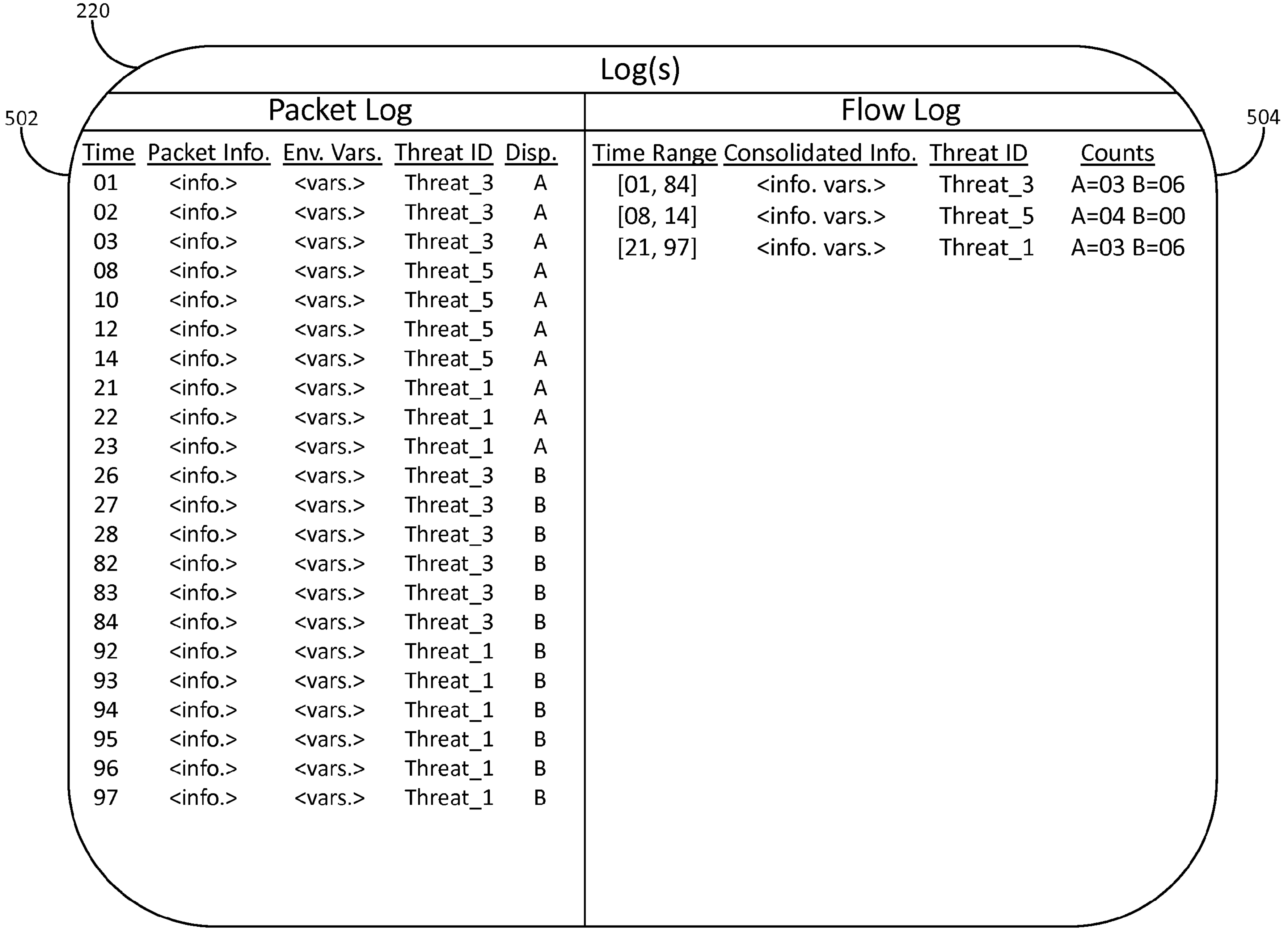
Packet Log

Time	Packet Info.	Env. Vars.	Threat ID	Disp.
01	<info.>	<vars.>	Threat_3	A
02	<info.>	<vars.>	Threat_3	A
03	<info.>	<vars.>	Threat_3	A
08	<info.>	<vars.>	Threat_5	A
10	<info.>	<vars.>	Threat_5	A
12	<info.>	<vars.>	Threat_5	A
14	<info.>	<vars.>	Threat_5	A
21	<info.>	<vars.>	Threat_1	A
22	<info.>	<vars.>	Threat_1	A
23	<info.>	<vars.>	Threat_1	A
26	<info.>	<vars.>	Threat_3	B
27	<info.>	<vars.>	Threat_3	B
28	<info.>	<vars.>	Threat_3	B
82	<info.>	<vars.>	Threat_3	B
83	<info.>	<vars.>	Threat_3	B
84	<info.>	<vars.>	Threat_3	B
92	<info.>	<vars.>	Threat_1	B
93	<info.>	<vars.>	Threat_1	B
94	<info.>	<vars.>	Threat_1	B
95	<info.>	<vars.>	Threat_1	B
96	<info.>	<vars.>	Threat_1	B
97	<info.>	<vars.>	Threat_1	B

Flow Log

Time Range	Consolidated Info.	Threat ID	Counts
[01, 84]	<info. vars.>	Threat_3	A=03 B=06
[08, 14]	<info. vars.>	Threat_5	A=04 B=00
[21, 23]	<info. vars.>	Threat_1	A=03 B=00

FIG. 5F


220
502
504
Log(s)

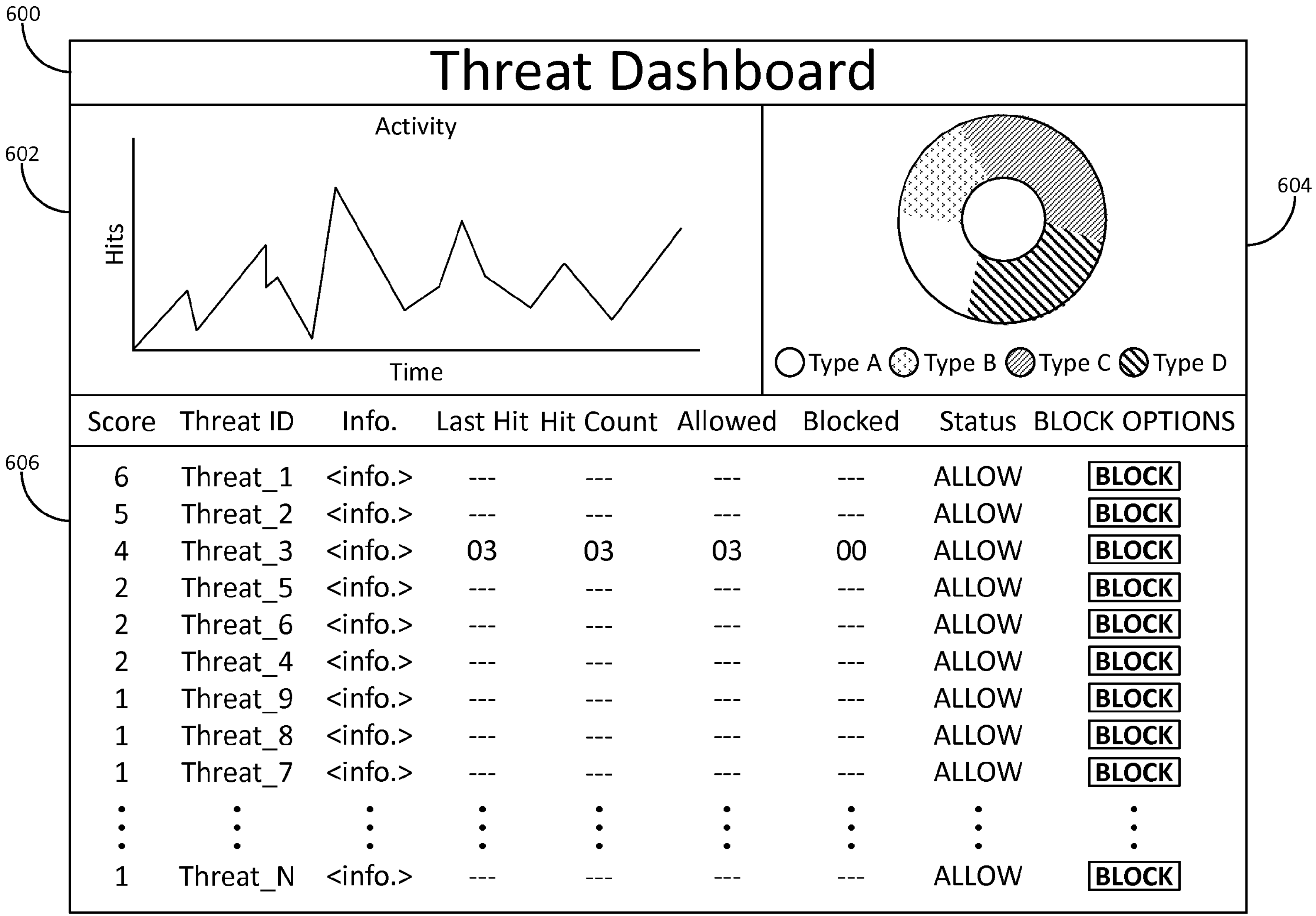
Packet Log

Time	Packet Info.	Env. Vars.	Threat ID	Disp.
01	<info.>	<vars.>	Threat_3	A
02	<info.>	<vars.>	Threat_3	A
03	<info.>	<vars.>	Threat_3	A
08	<info.>	<vars.>	Threat_5	A
10	<info.>	<vars.>	Threat_5	A
12	<info.>	<vars.>	Threat_5	A
14	<info.>	<vars.>	Threat_5	A
21	<info.>	<vars.>	Threat_1	A
22	<info.>	<vars.>	Threat_1	A
23	<info.>	<vars.>	Threat_1	A
26	<info.>	<vars.>	Threat_3	B
27	<info.>	<vars.>	Threat_3	B
28	<info.>	<vars.>	Threat_3	B
82	<info.>	<vars.>	Threat_3	B
83	<info.>	<vars.>	Threat_3	B
84	<info.>	<vars.>	Threat_3	B
92	<info.>	<vars.>	Threat_1	B
93	<info.>	<vars.>	Threat_1	B
94	<info.>	<vars.>	Threat_1	B
95	<info.>	<vars.>	Threat_1	B
96	<info.>	<vars.>	Threat_1	B
97	<info.>	<vars.>	Threat_1	B

Flow Log

Time Range	Consolidated Info.	Threat ID	Counts
[01, 84]	<info. vars.>	Threat_3	A=03 B=06
[08, 14]	<info. vars.>	Threat_5	A=04 B=00
[21, 97]	<info. vars.>	Threat_1	A=03 B=06

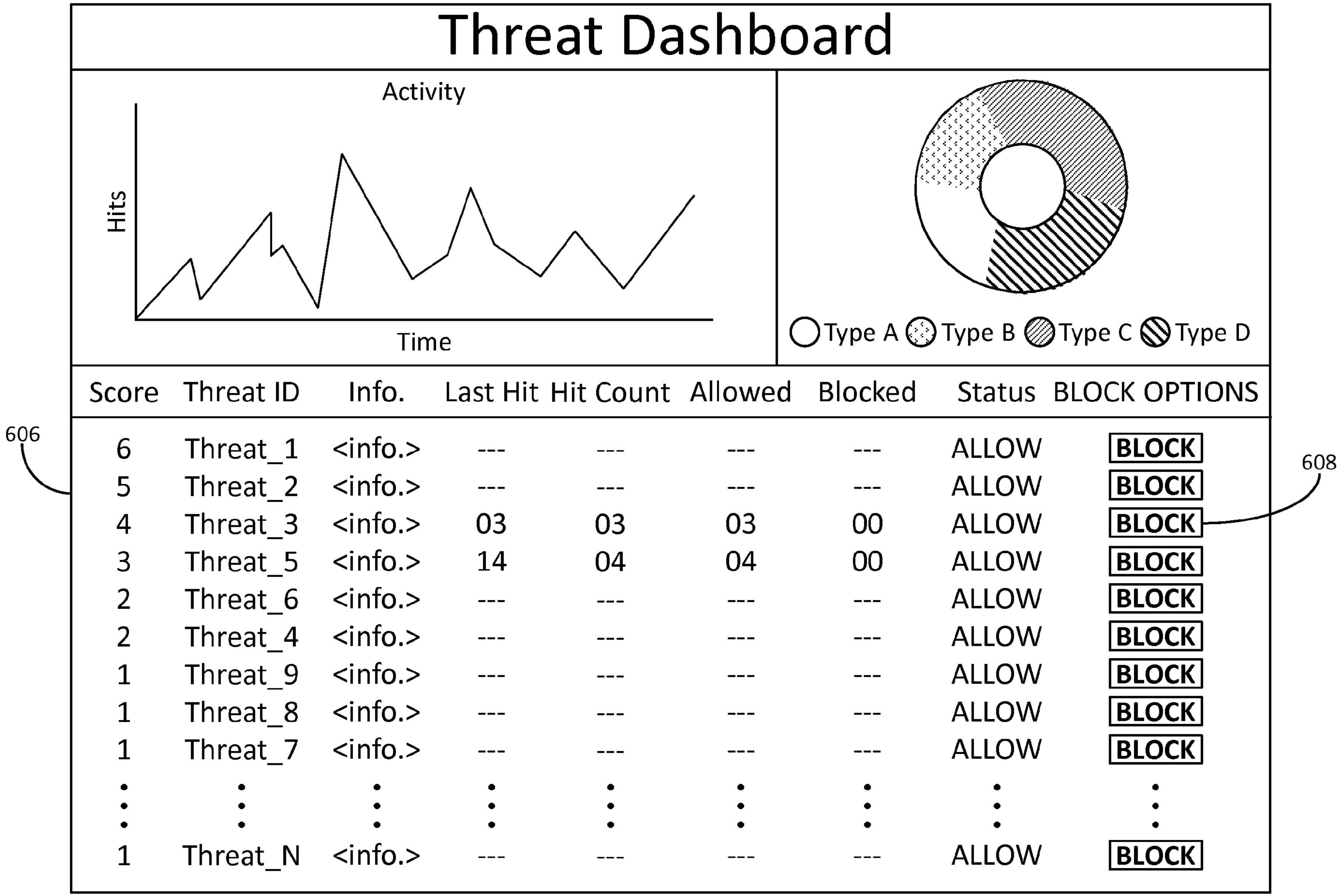
FIG. 5G



Threat Dashboard

Score	Threat ID	Info.	Last Hit	Hit Count	Allowed	Blocked	Status	BLOCK OPTIONS
6	Threat_1	<info.>	---	---	---	---	ALLOW	BLOCK
5	Threat_2	<info.>	---	---	---	---	ALLOW	BLOCK
4	Threat_3	<info.>	03	03	03	00	ALLOW	BLOCK
2	Threat_5	<info.>	---	---	---	---	ALLOW	BLOCK
2	Threat_6	<info.>	---	---	---	---	ALLOW	BLOCK
2	Threat_4	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_9	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_8	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_7	<info.>	---	---	---	---	ALLOW	BLOCK
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	Threat_N	<info.>	---	---	---	---	ALLOW	BLOCK

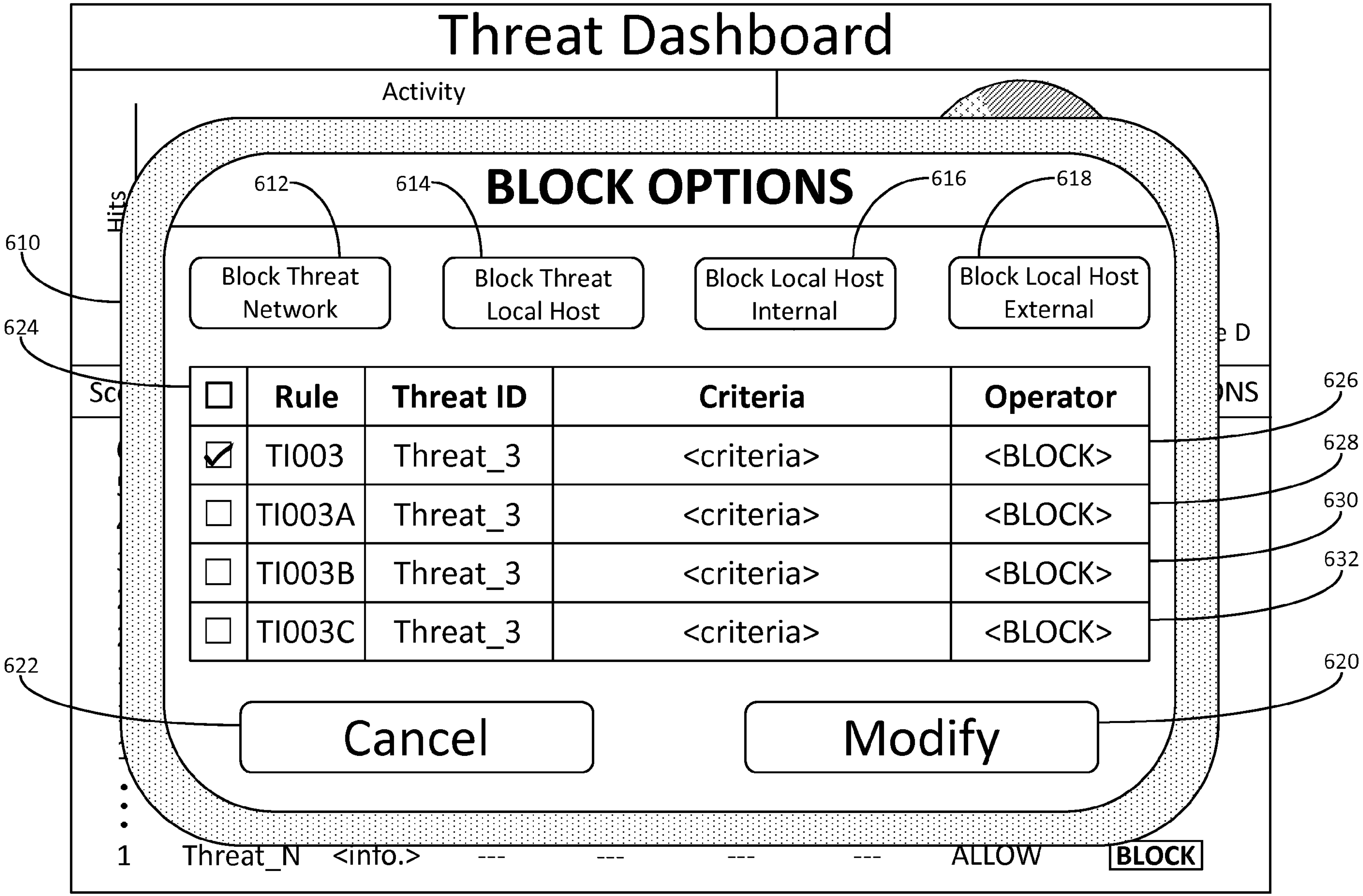
FIG. 6A



Threat Dashboard

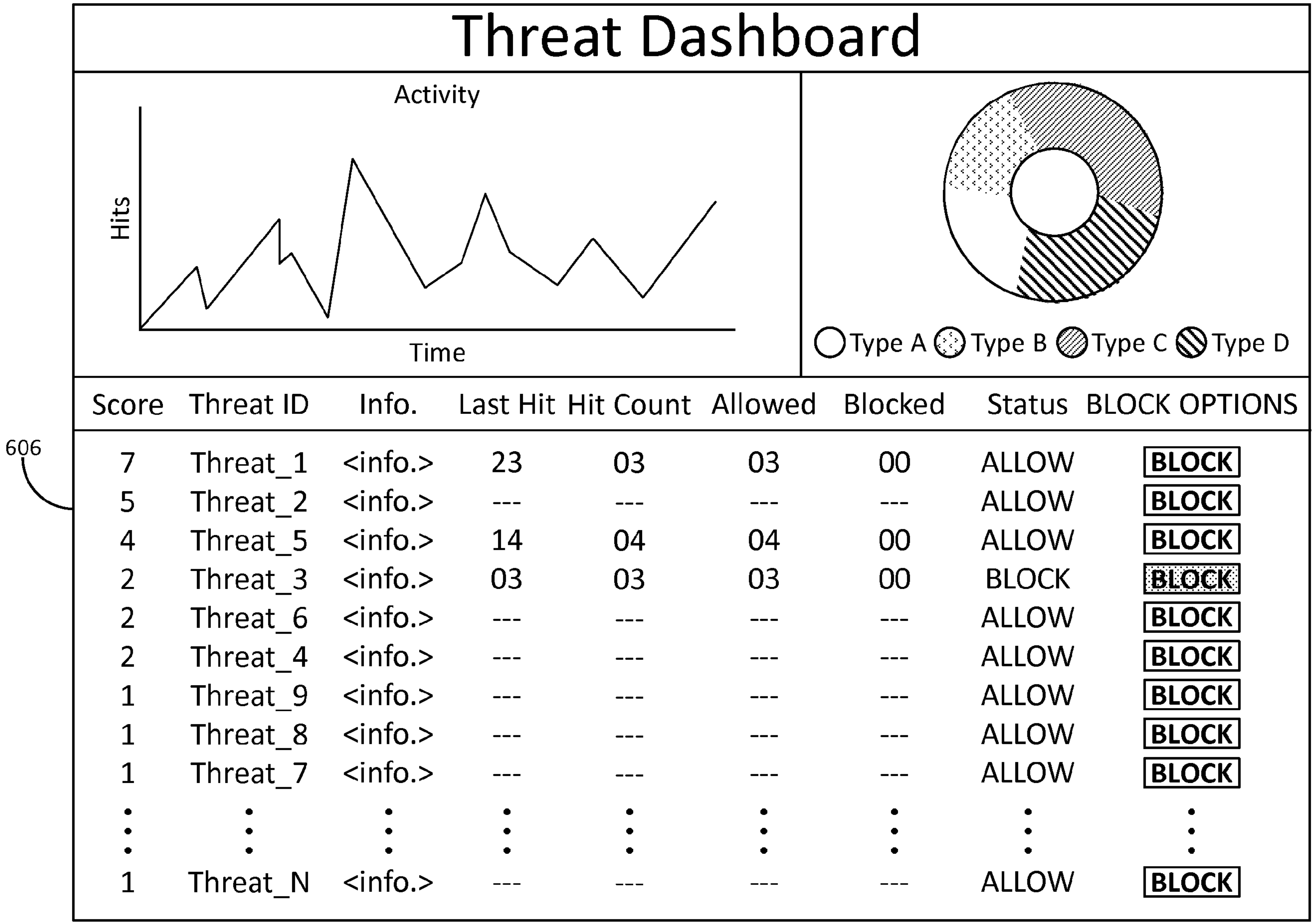
Score	Threat ID	Info.	Last Hit	Hit Count	Allowed	Blocked	Status	BLOCK OPTIONS
6	Threat_1	<info.>	---	---	---	---	ALLOW	BLOCK
5	Threat_2	<info.>	---	---	---	---	ALLOW	BLOCK
4	Threat_3	<info.>	03	03	03	00	ALLOW	BLOCK
3	Threat_5	<info.>	14	04	04	00	ALLOW	BLOCK
2	Threat_6	<info.>	---	---	---	---	ALLOW	BLOCK
2	Threat_4	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_9	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_8	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_7	<info.>	---	---	---	---	ALLOW	BLOCK
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	Threat_N	<info.>	---	---	---	---	ALLOW	BLOCK

FIG. 6B



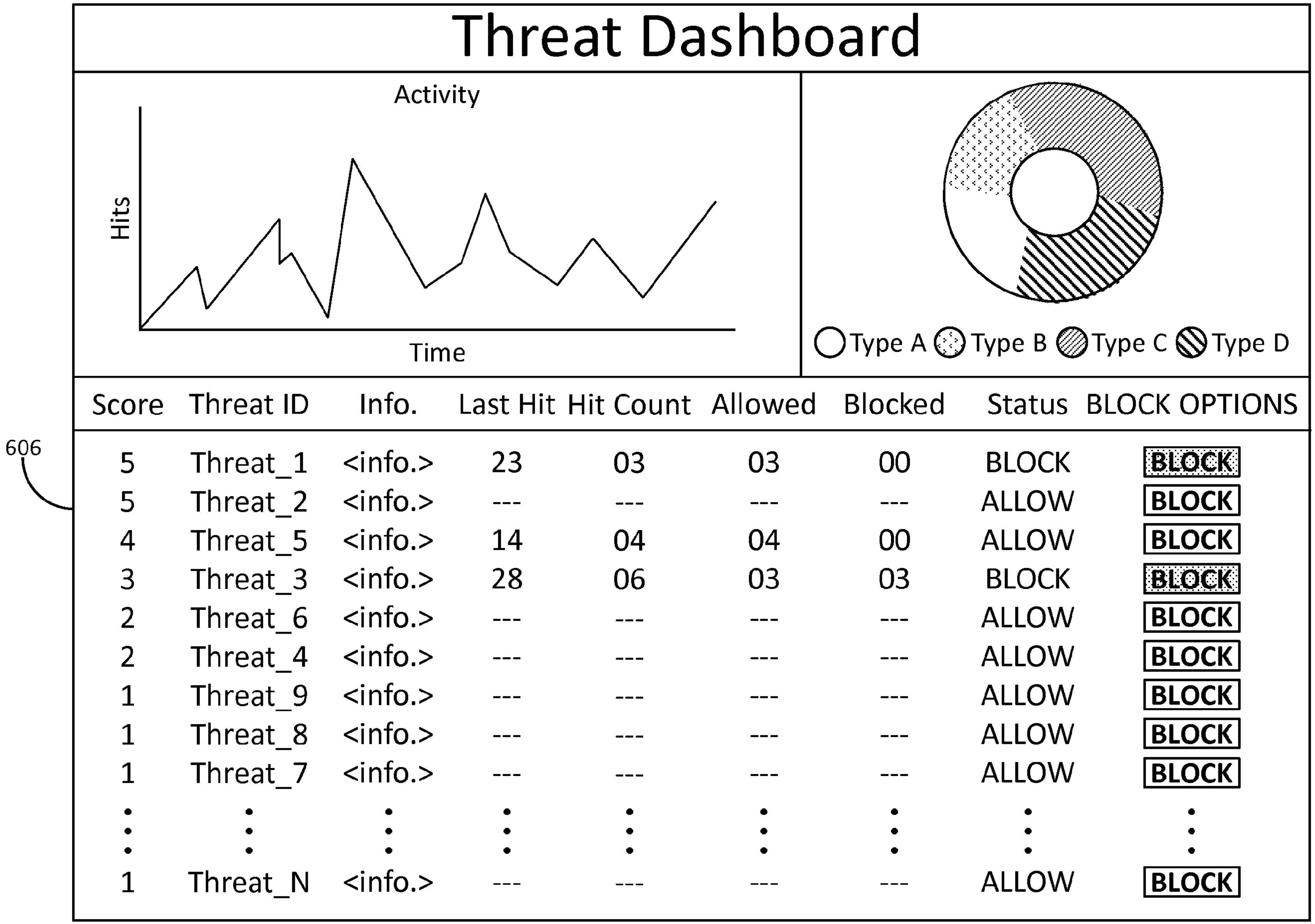
□	Rule	Threat ID	Criteria	Operator
☑	TI003	Threat_3	<criteria>	<BLOCK>
□	TI003A	Threat_3	<criteria>	<BLOCK>
□	TI003B	Threat_3	<criteria>	<BLOCK>
□	TI003C	Threat_3	<criteria>	<BLOCK>

FIG. 6C



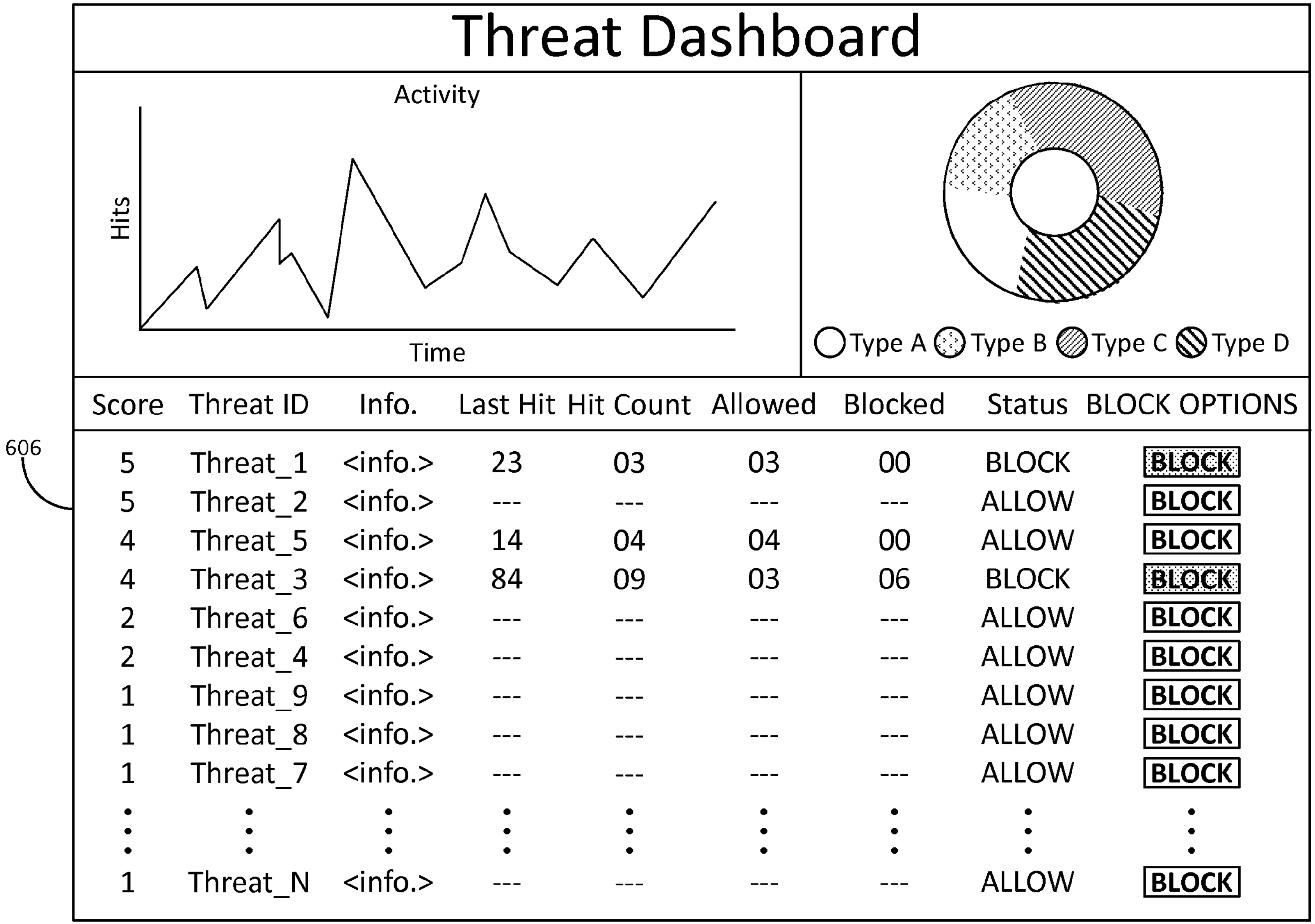
Score	Threat ID	Info.	Last Hit	Hit Count	Allowed	Blocked	Status	BLOCK OPTIONS
7	Threat_1	<info.>	23	03	03	00	ALLOW	BLOCK
5	Threat_2	<info.>	---	---	---	---	ALLOW	BLOCK
4	Threat_5	<info.>	14	04	04	00	ALLOW	BLOCK
2	Threat_3	<info.>	03	03	03	00	BLOCK	BLOCK
2	Threat_6	<info.>	---	---	---	---	ALLOW	BLOCK
2	Threat_4	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_9	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_8	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_7	<info.>	---	---	---	---	ALLOW	BLOCK
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	Threat_N	<info.>	---	---	---	---	ALLOW	BLOCK

FIG. 6D



Score	Threat ID	Info.	Last Hit	Hit Count	Allowed	Blocked	Status	BLOCK OPTIONS
5	Threat_1	<info.>	23	03	03	00	BLOCK	BLOCK
5	Threat_2	<info.>	---	---	---	---	ALLOW	BLOCK
4	Threat_5	<info.>	14	04	04	00	ALLOW	BLOCK
3	Threat_3	<info.>	28	06	03	03	BLOCK	BLOCK
2	Threat_6	<info.>	---	---	---	---	ALLOW	BLOCK
2	Threat_4	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_9	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_8	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_7	<info.>	---	---	---	---	ALLOW	BLOCK
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	Threat_N	<info.>	---	---	---	---	ALLOW	BLOCK

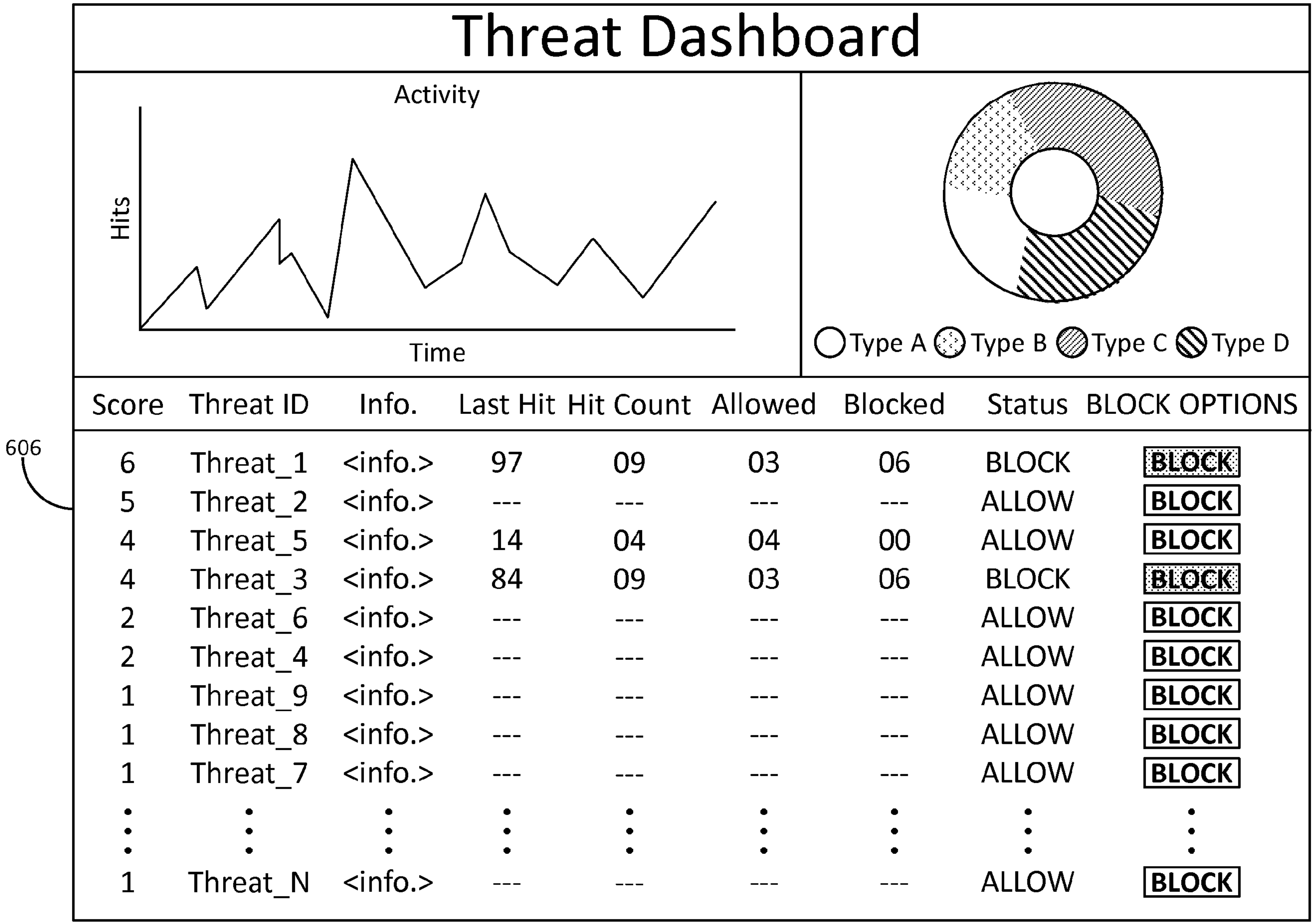
FIG. 6E



Threat Dashboard

Score	Threat ID	Info.	Last Hit	Hit Count	Allowed	Blocked	Status	BLOCK OPTIONS
5	Threat_1	<info.>	23	03	03	00	BLOCK	BLOCK
5	Threat_2	<info.>	---	---	---	---	ALLOW	BLOCK
4	Threat_5	<info.>	14	04	04	00	ALLOW	BLOCK
4	Threat_3	<info.>	84	09	03	06	BLOCK	BLOCK
2	Threat_6	<info.>	---	---	---	---	ALLOW	BLOCK
2	Threat_4	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_9	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_8	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_7	<info.>	---	---	---	---	ALLOW	BLOCK
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	Threat_N	<info.>	---	---	---	---	ALLOW	BLOCK

FIG. 6F



Score	Threat ID	Info.	Last Hit	Hit Count	Allowed	Blocked	Status	BLOCK OPTIONS
6	Threat_1	<info.>	97	09	03	06	BLOCK	BLOCK
5	Threat_2	<info.>	---	---	---	---	ALLOW	BLOCK
4	Threat_5	<info.>	14	04	04	00	ALLOW	BLOCK
4	Threat_3	<info.>	84	09	03	06	BLOCK	BLOCK
2	Threat_6	<info.>	---	---	---	---	ALLOW	BLOCK
2	Threat_4	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_9	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_8	<info.>	---	---	---	---	ALLOW	BLOCK
1	Threat_7	<info.>	---	---	---	---	ALLOW	BLOCK
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	Threat_N	<info.>	---	---	---	---	ALLOW	BLOCK

FIG. 6G

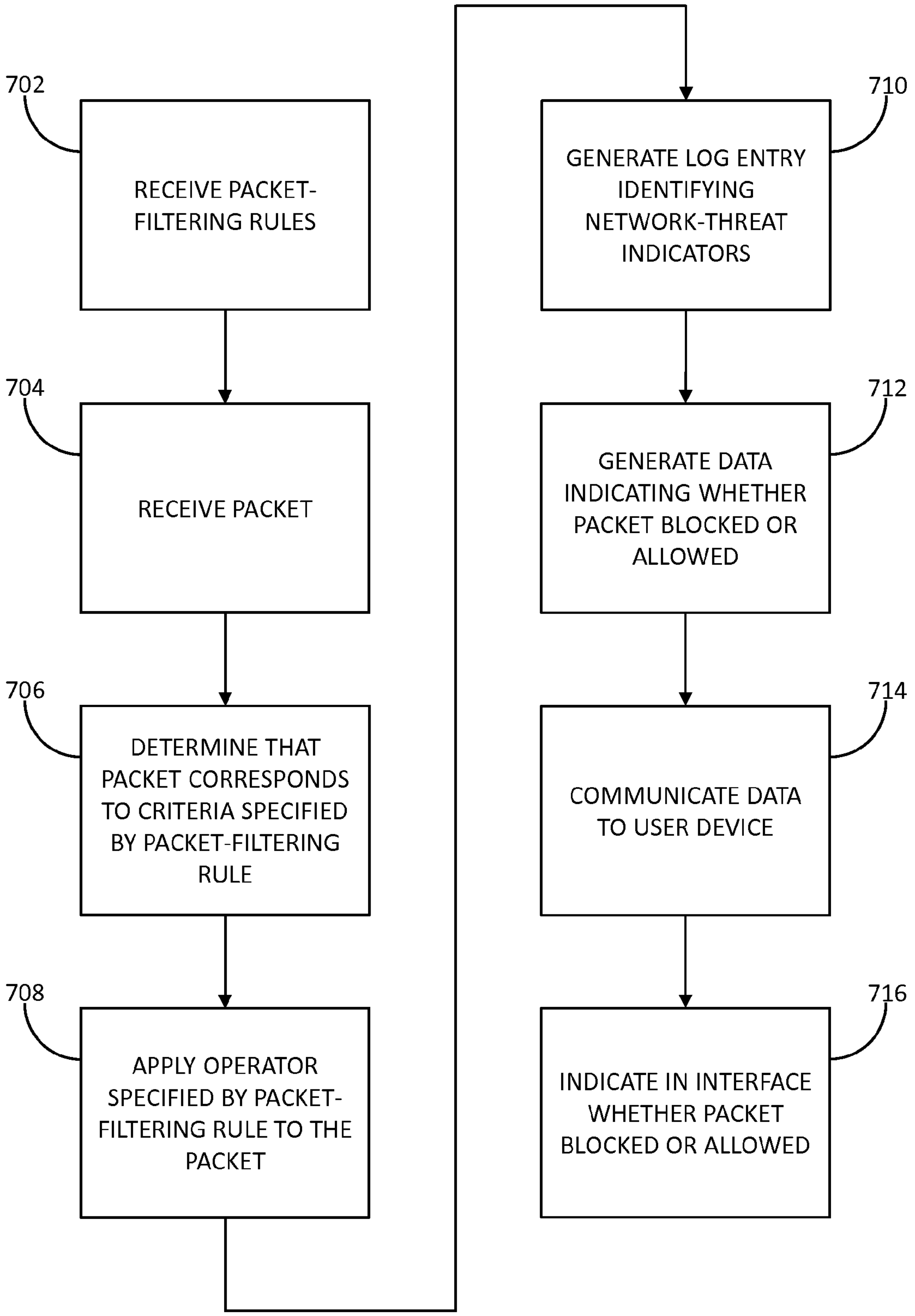

702
RECEIVE PACKET-FILTERING RULES
704
RECEIVE PACKET
706
DETERMINE THAT PACKET CORRESPONDS TO CRITERIA SPECIFIED BY PACKET-FILTERING RULE
708
APPLY OPERATOR SPECIFIED BY PACKET-FILTERING RULE TO THE PACKET
710
GENERATE LOG ENTRY IDENTIFYING NETWORK-THREAT INDICATORS
712
GENERATE DATA INDICATING WHETHER PACKET BLOCKED OR ALLOWED
714
COMMUNICATE DATA TO USER DEVICE
716
INDICATE IN INTERFACE WHETHER PACKET BLOCKED OR ALLOWED

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/026339

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L12/26
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2004/093513 A1 (CANTRELL CRAIG [US] ET AL) 13 May 2004 (2004-05-13) abstract paragraph [0012] - paragraph [0044]; figure 1 paragraph [0065] - paragraph [0069] -----	1,31,32 2-30, 33-43
X Y	US 2012/023576 A1 (SORENSEN AMANDA [US] ET AL) 26 January 2012 (2012-01-26) abstract paragraph [0006] - paragraph [0012]; figure 3 -----	1,31,32 2-30, 33-43
X A	US 2008/163333 A1 (KASRALIKAR RAHUL [US]) 3 July 2008 (2008-07-03) abstract paragraph [0009] - paragraph [0010]; figure 2 -----	1,31,32 2-30, 33-43

□ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 1 June 2016	Date of mailing of the international search report 09/06/2016
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer San Millán Maeso, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/026339

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004093513 A1	13-05-2004	AR 042020 A1	08-06-2005
		AU 2003290674 A1	03-06-2004
		CN 1720459 A	11-01-2006
		EP 1558937 A2	03-08-2005
		JP 2006506853 A	23-02-2006
		JP 2010268483 A	25-11-2010
		KR 20050086441 A	30-08-2005
		KR 20100132079 A	16-12-2010
		US 2004093513 A1	13-05-2004
		US 2005028013 A1	03-02-2005
		US 2005044422 A1	24-02-2005
		WO 2004045126 A2	27-05-2004
US 2012023576 A1	26-01-2012	AU 2011279907 A1	28-02-2013
		CA 2805823 A1	26-01-2012
		SG 187068 A1	28-02-2013
		US 2012023576 A1	26-01-2012
		WO 2012012280 A2	26-01-2012
US 2008163333 A1	03-07-2008	NONE	