US 20100257580A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2010/0257580 A1**

(43) **Pub. Date: Oct. 7, 2010**

ZHAO

(54) **BEHAVIOR-BASED TRAFFIC PROFILING BASED ON ACCESS CONTROL INFORMATION**

(75) Inventor: **Ye (Kevin) ZHAO**, Beijing (CN)

Correspondence Address:
HARRITY & HARRITY, LLP
11350 Random Hills Road, SUITE 600
FAIRFAX, VA 22030 (US)

(73) Assignee: **Juniper Networks, Inc.**, Sunnyvale, CA (US)

(21) Appl. No.: **12/476,567**

(22) Filed: **Jun. 2, 2009**

(30) **Foreign Application Priority Data**

Apr. 3, 2009 (CN) 200910130365.5

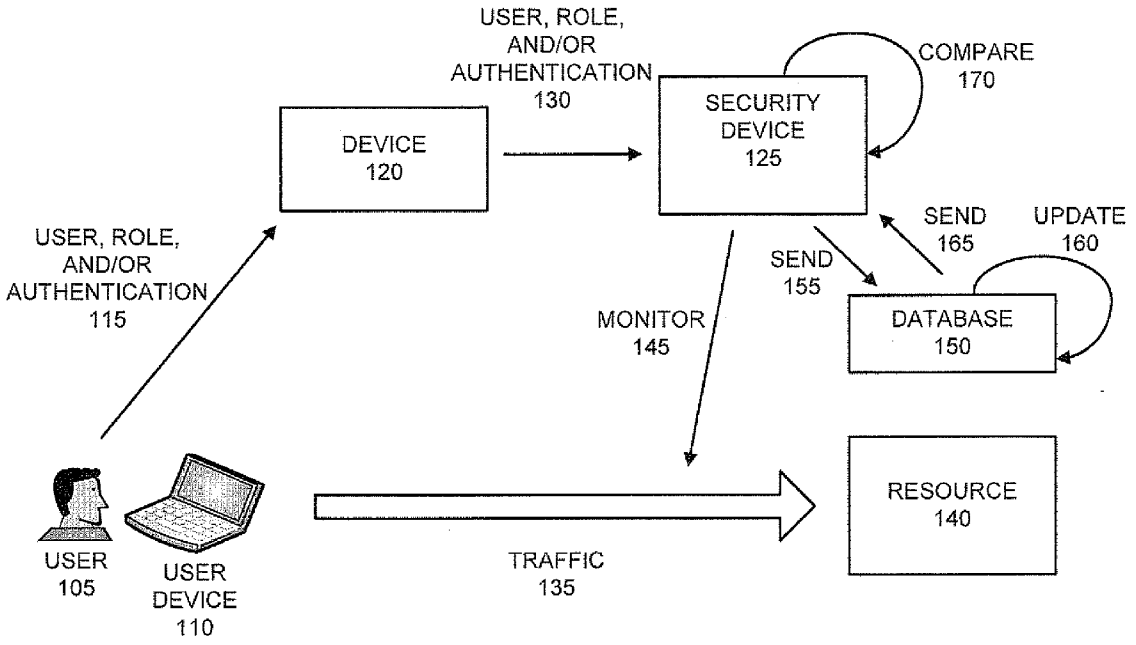
Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)
G06F 11/00 (2006.01)

(52) **U.S. Cl.** **726/1**; 726/23

(57) **ABSTRACT**

A method includes receiving one or more of user information, role information, or authorization information associated with a user accessing a network, selecting a traffic flow to monitor that is associated with the one or more of user information, role information, or authorization information, monitoring the traffic flow, determining whether an anomaly exists with respect to the traffic flow based on a traffic behavior pattern associated with the one or more of user information, role information, or authorization information, and performing a security response when it is determined that the anomaly exists.



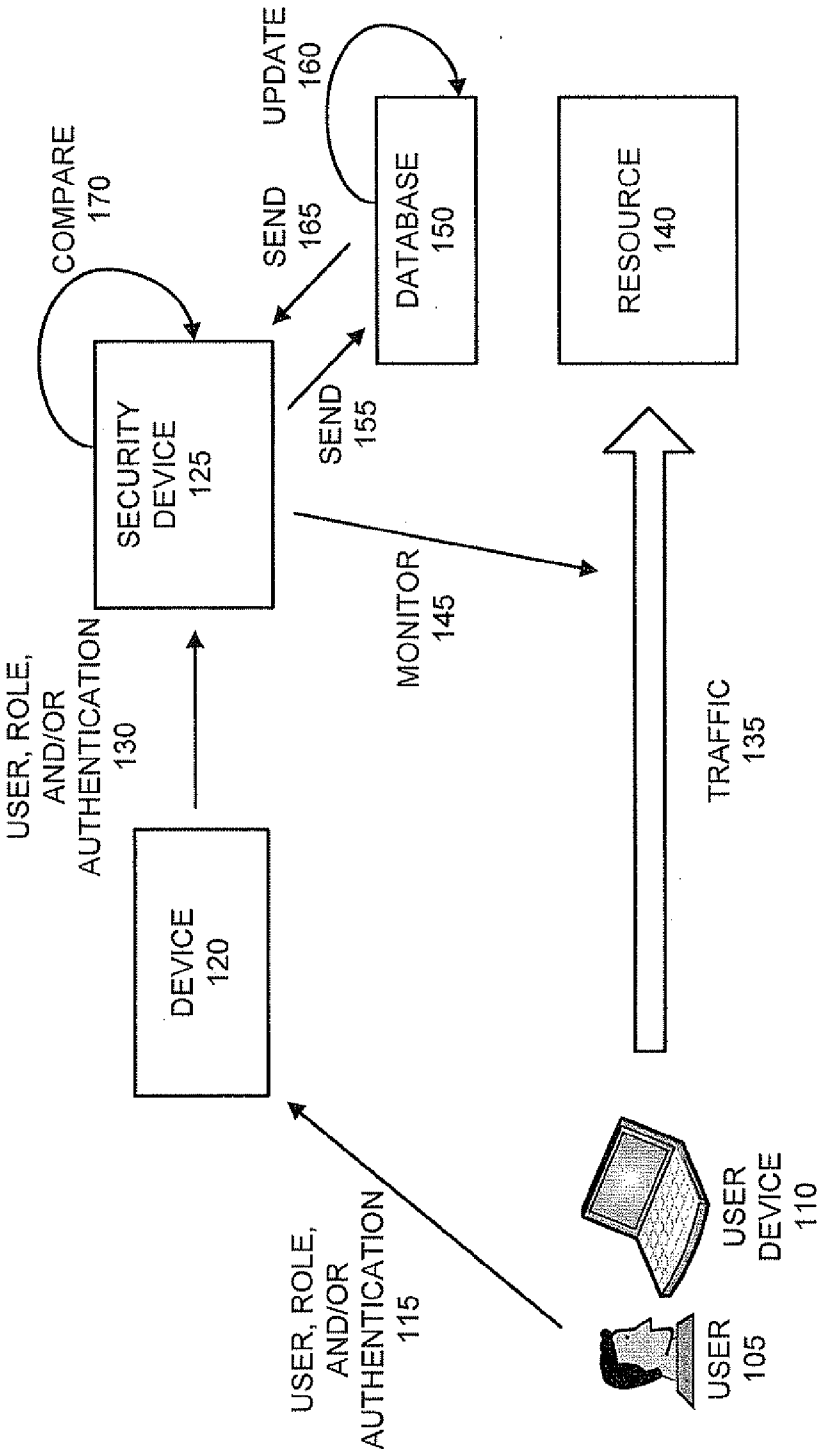

USER
105
USER DEVICE
110
USER, ROLE, AND/OR AUTHENTICATION
115
DEVICE
120
USER, ROLE, AND/OR AUTHENTICATION
130
SECURITY DEVICE
125
COMPARE
170
SEND
165
UPDATE
160
DATABASE
150
SEND
155
MONITOR
145
TRAFFIC
135
RESOURCE
140

FIG. 1A

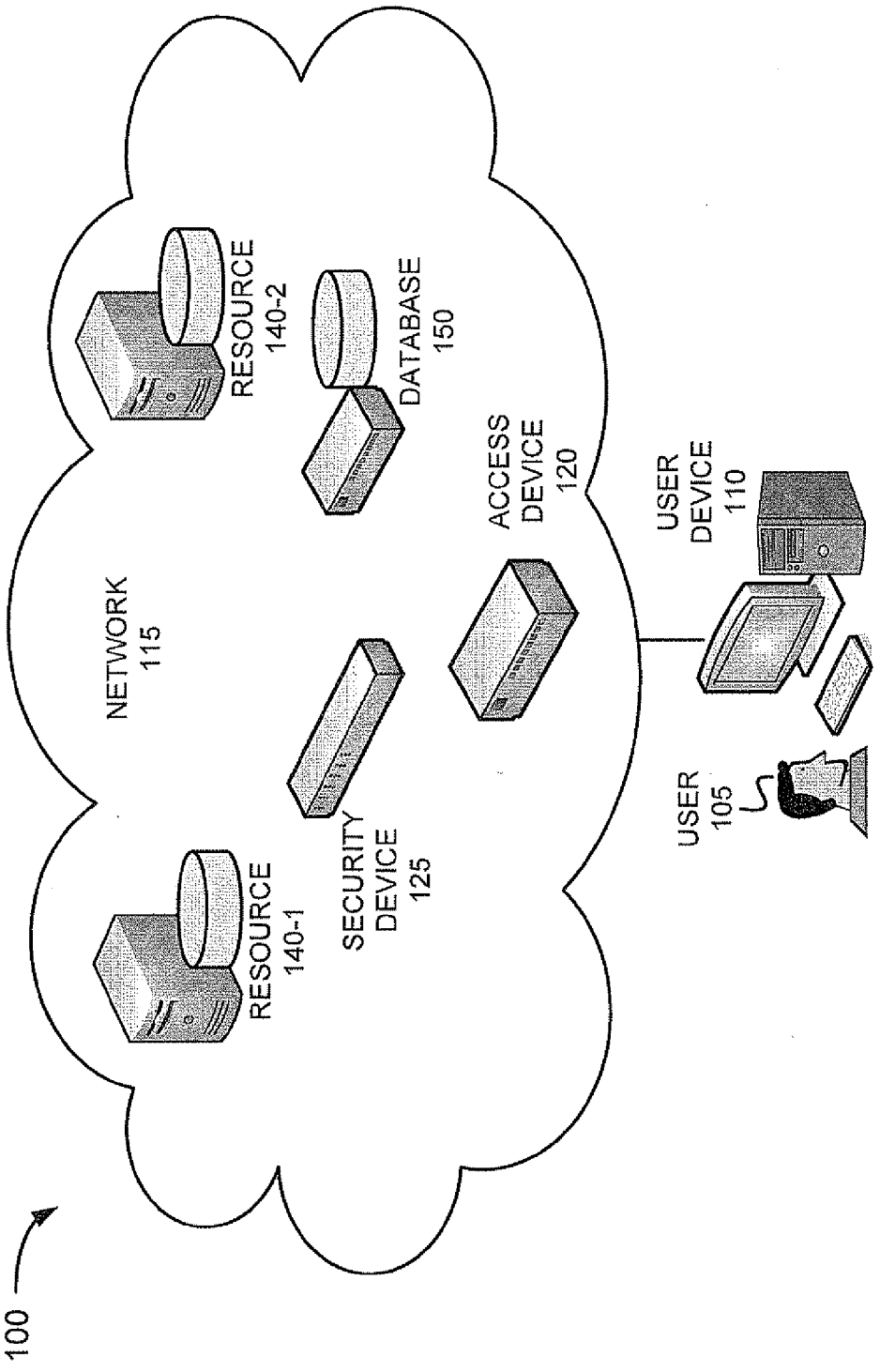

100
NETWORK
115
RESOURCE
140-1
SECURITY
DEVICE
125
RESOURCE
140-2
DATABASE
150
ACCESS
DEVICE
120
USER
DEVICE
110
USER
105

FIG. 1B

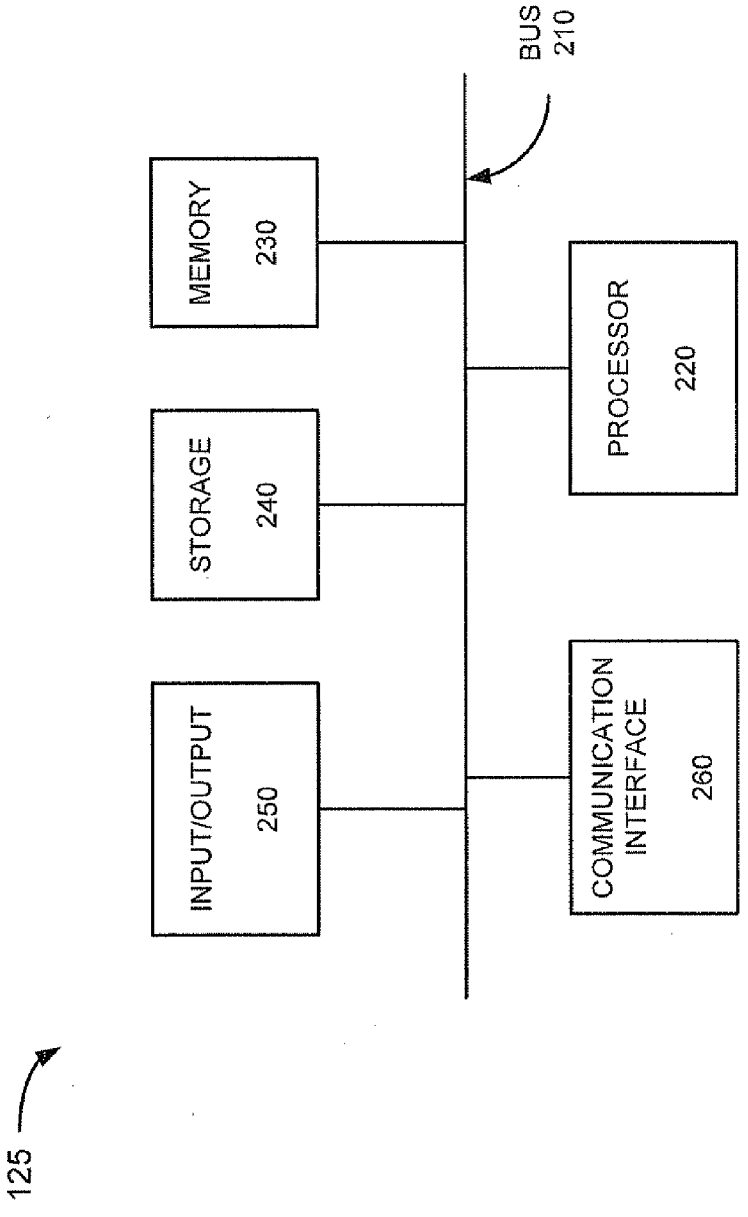

125
BUS
210
MEMORY
230
STORAGE
240
INPUT/OUTPUT
250
PROCESSOR
220
COMMUNICATION
INTERFACE
260

FIG. 2

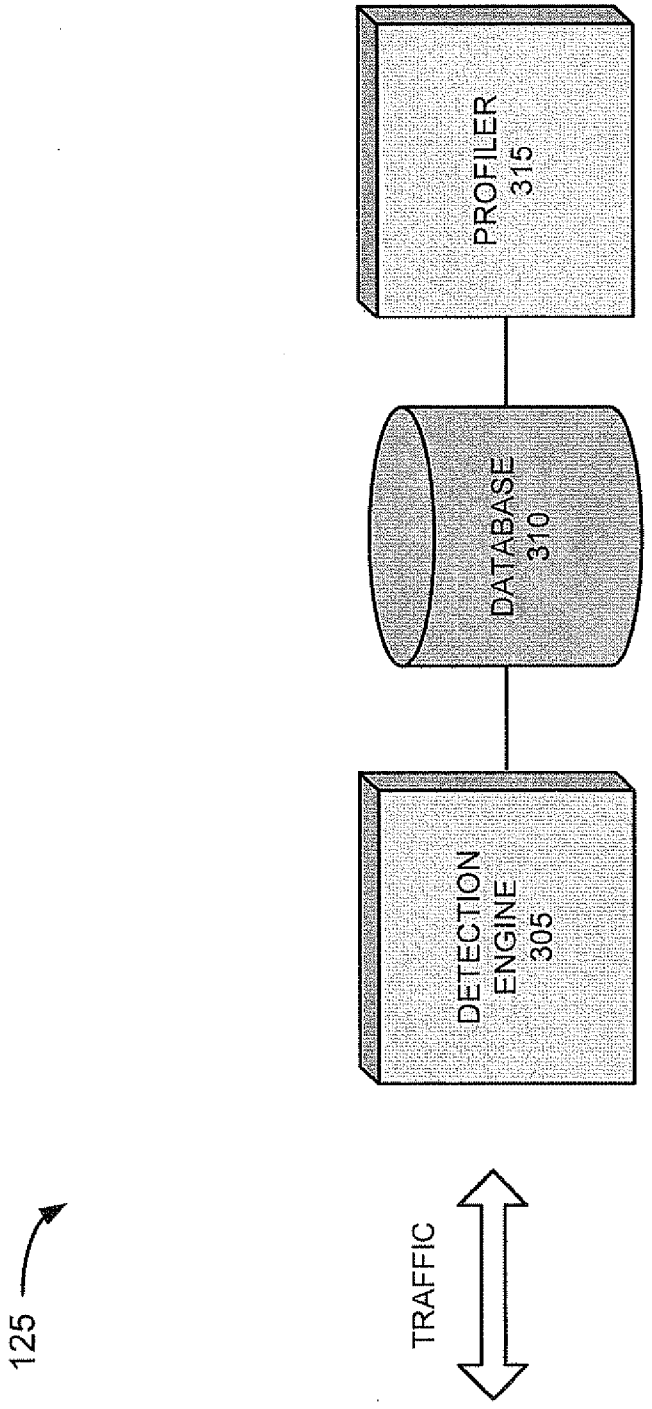

125
TRAFFIC
DETECTION ENGINE 305
DATABASE 310
PROFILER 315

FIG. 3

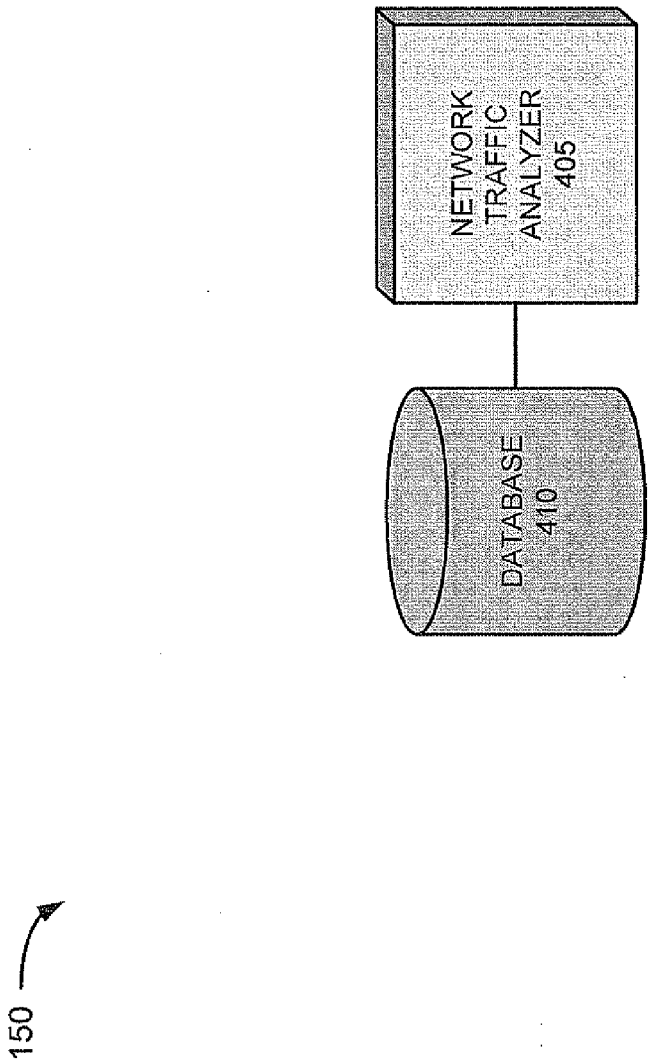


FIG. 4A

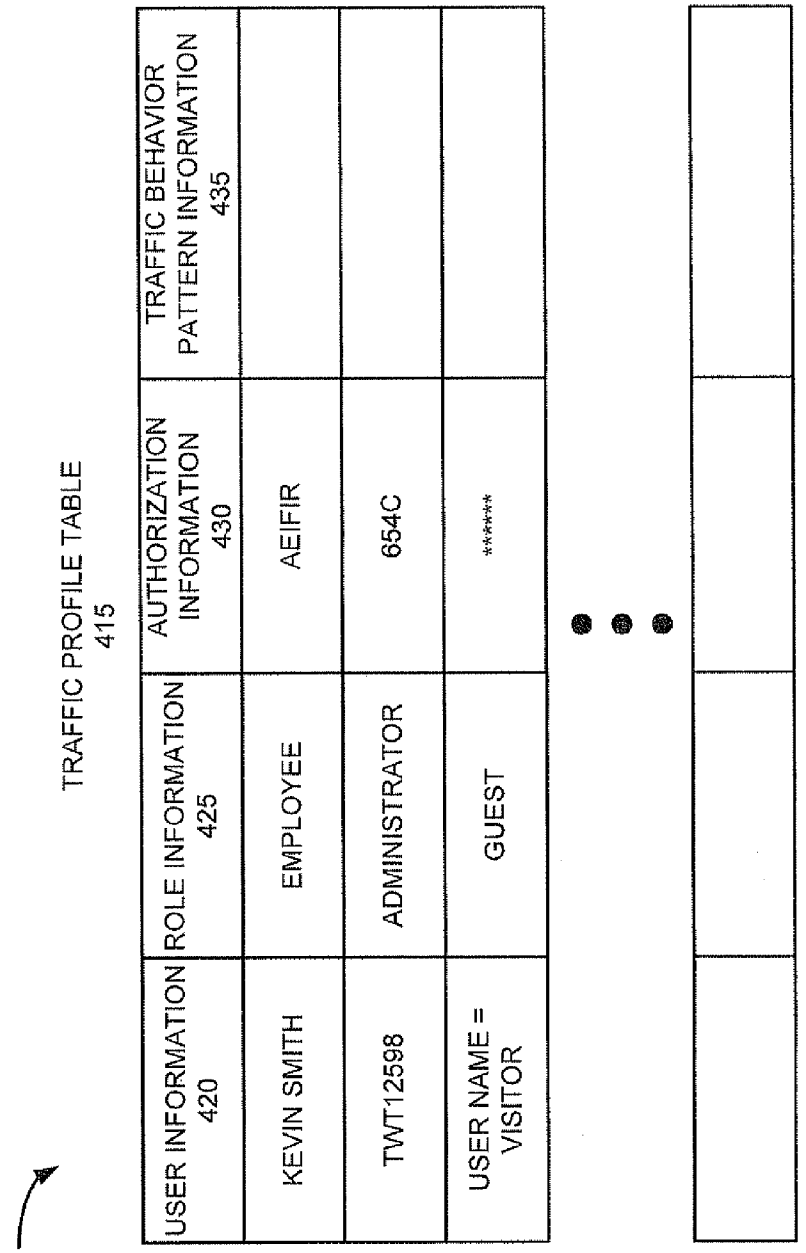

410
TRAFFIC PROFILE TABLE
415
USER INFORMATION 420
ROLE INFORMATION 425
AUTHORIZATION INFORMATION 430
TRAFFIC BEHAVIOR PATTERN INFORMATION 435
KEVIN SMITH
EMPLOYEE
AEIFIR
TWT12598
ADMINISTRATOR
654C
USER NAME = VISITOR
GUEST
******

FIG. 4B

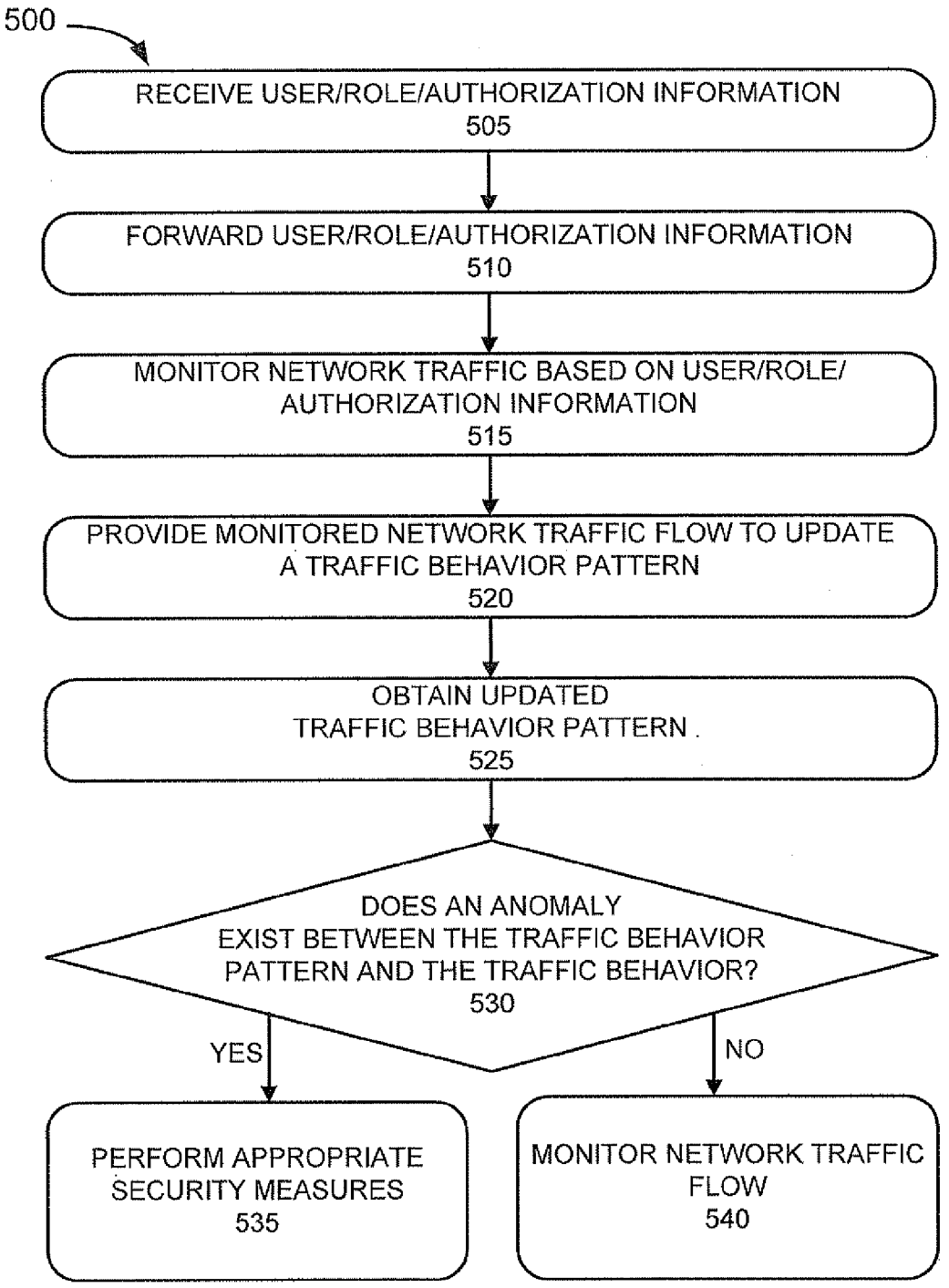

500
RECEIVE USER/ROLE/AUTHORIZATION INFORMATION
505
FORWARD USER/ROLE/AUTHORIZATION INFORMATION
510
MONITOR NETWORK TRAFFIC BASED ON USER/ROLE/
AUTHORIZATION INFORMATION
515
PROVIDE MONITORED NETWORK TRAFFIC FLOW TO UPDATE
A TRAFFIC BEHAVIOR PATTERN
520
OBTAIN UPDATED
TRAFFIC BEHAVIOR PATTERN
525
DOES AN ANOMALY
EXIST BETWEEN THE TRAFFIC BEHAVIOR
PATTERN AND THE TRAFFIC BEHAVIOR?
530
YES
NO
PERFORM APPROPRIATE
SECURITY MEASURES
535
MONITOR NETWORK TRAFFIC
FLOW
540

FIG. 5A

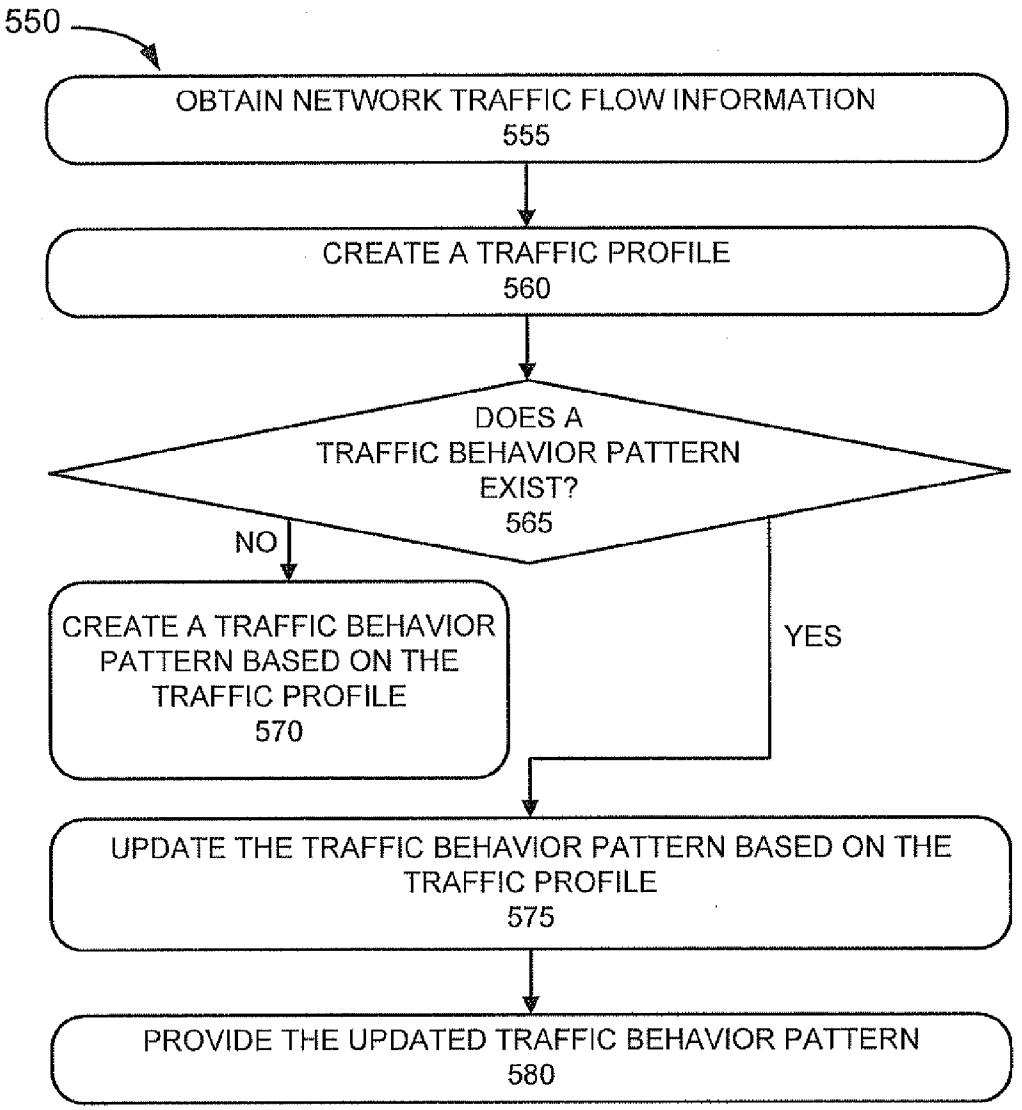

550
OBTAIN NETWORK TRAFFIC FLOW INFORMATION
555
CREATE A TRAFFIC PROFILE
560
DOES A TRAFFIC BEHAVIOR PATTERN EXIST?
565
NO
YES
CREATE A TRAFFIC BEHAVIOR PATTERN BASED ON THE TRAFFIC PROFILE
570
UPDATE THE TRAFFIC BEHAVIOR PATTERN BASED ON THE TRAFFIC PROFILE
575
PROVIDE THE UPDATED TRAFFIC BEHAVIOR PATTERN
580

FIG. 5B

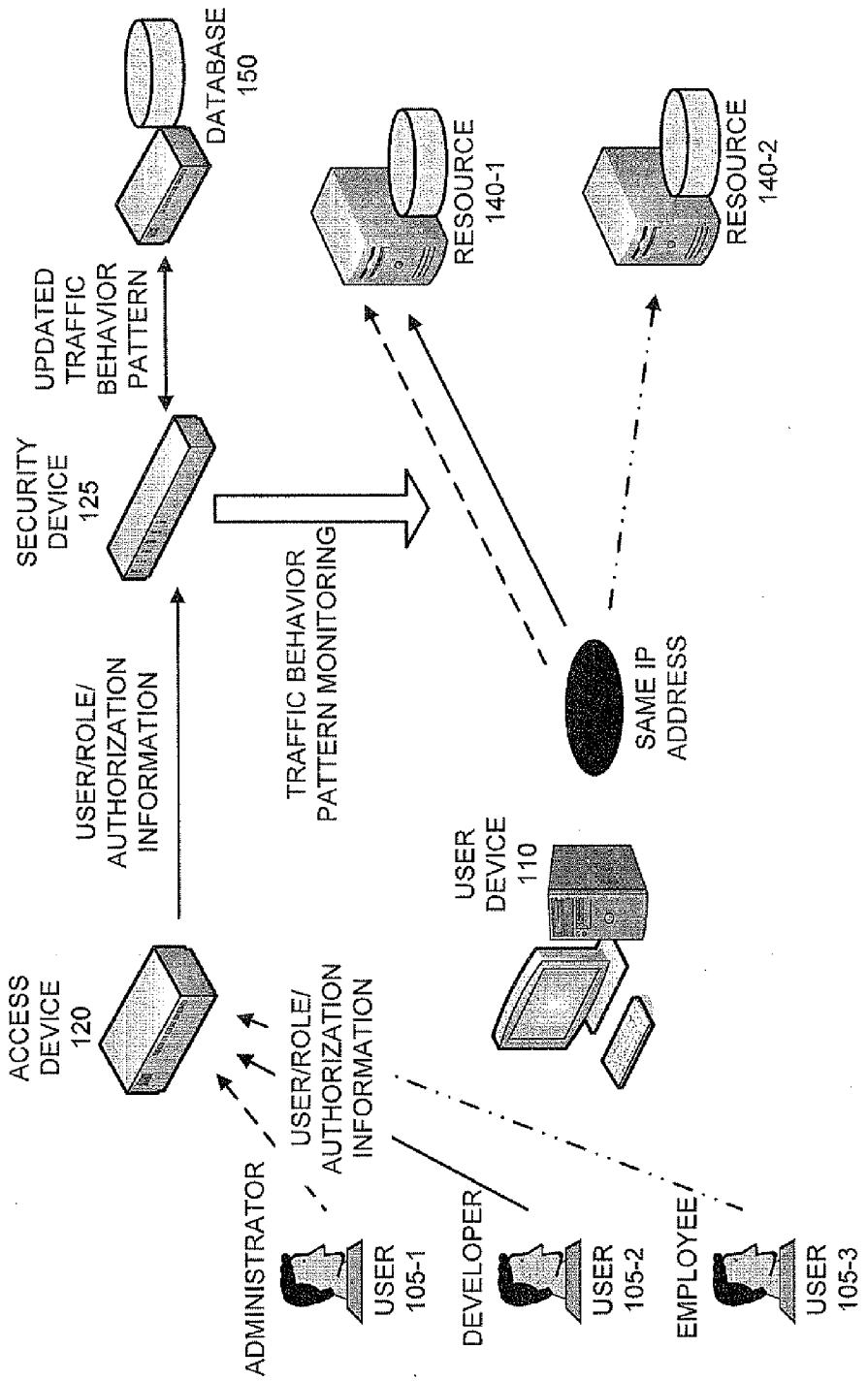

ADMINISTRATOR
USER 105-1
DEVELOPER
USER 105-2
EMPLOYEE
USER 105-3
USER/ROLE/ AUTHORIZATION INFORMATION
ACCESS DEVICE 120
USER/ROLE/ AUTHORIZATION INFORMATION
SECURITY DEVICE 125
UPDATED TRAFFIC BEHAVIOR PATTERN
DATABASE 150
TRAFFIC BEHAVIOR PATTERN MONITORING
USER DEVICE 110
SAME IP ADDRESS
RESOURCE 140-1
RESOURCE 140-2

FIG. 6

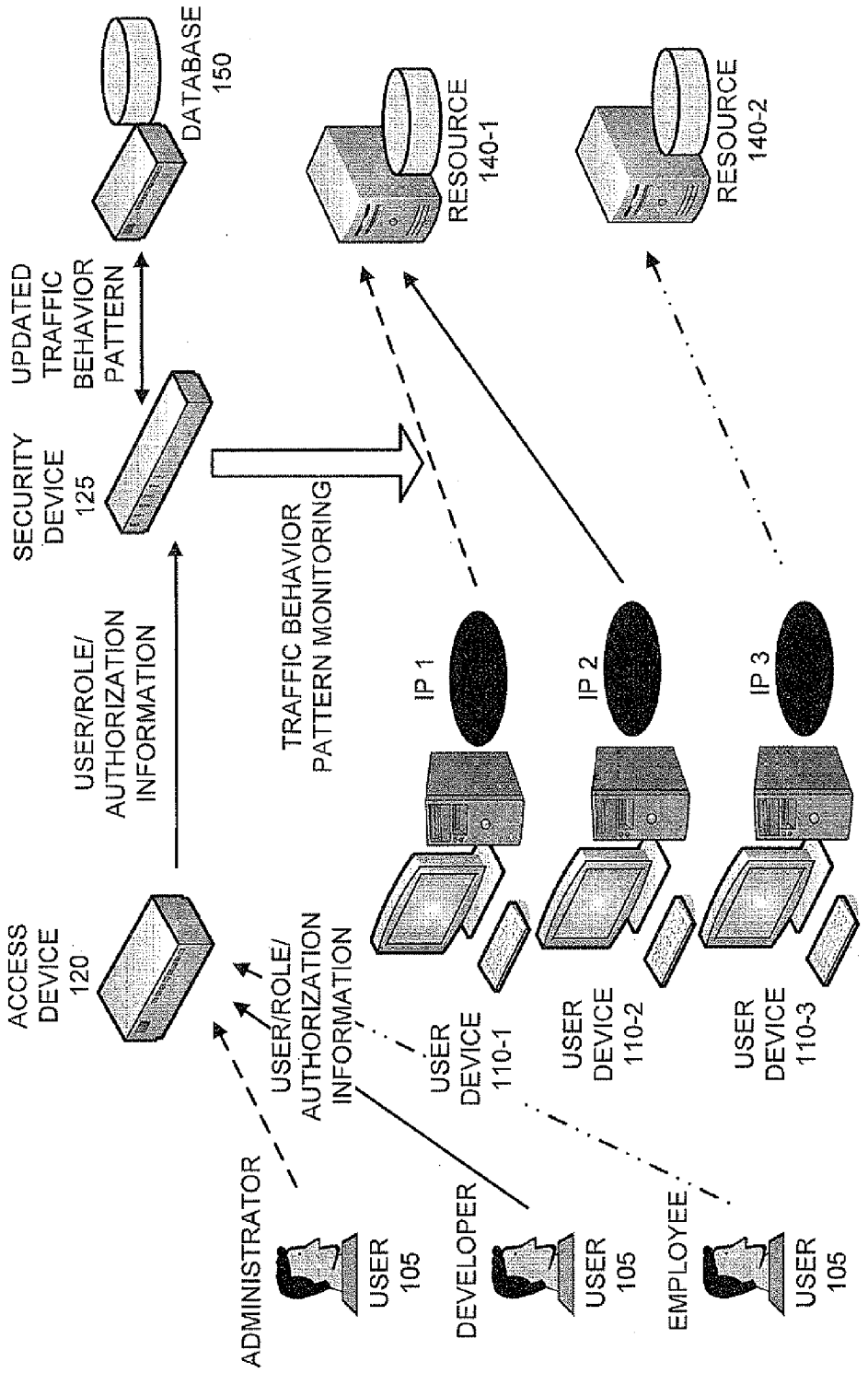

DATABASE 150
UPDATED TRAFFIC BEHAVIOR PATTERN
SECURITY DEVICE 125
RESOURCE 140-1
RESOURCE 140-2
USER/ROLE/ AUTHORIZATION INFORMATION
TRAFFIC BEHAVIOR PATTERN MONITORING
IP 1
IP 2
IP 3
ACCESS DEVICE 120
USER/ROLE/ AUTHORIZATION INFORMATION
USER DEVICE 110-1
USER DEVICE 110-2
USER DEVICE 110-3
ADMINISTRATOR
DEVELOPER
EMPLOYEE
USER 105
USER 105
USER 105

FIG. 7

BEHAVIOR-BASED TRAFFIC PROFILING BASED ON ACCESS CONTROL INFORMATION

BACKGROUND

[0001] Security devices, such as intrusion detection and prevention (IDP) devices, have become a key component in both service provider and enterprise networks. Mitigation is often achieved through the policies of the security solutions deployed in the network. The security policies dictate what traffic is and what traffic is not a threat, malicious, and/or an attack, by defining a series of characteristics that, when matched by the traffic, represent traffic that should be allowed or denied.

SUMMARY

[0002] According to one implementation, a method, performed by a device, may include receiving, by the device, one or more of user information, role information, or authorization information associated with a user accessing a network, selecting, by the device, a traffic flow to monitor that is associated with the one or more of user information, role information, or authorization information, monitoring, by the device, the traffic flow, determining, by the device, whether an anomaly of traffic behavior exists with respect to the traffic flow based on a traffic behavior pattern associated with the one or more of user information, role information, or authorization information, and performing, by the device, a security response when it is determined that the anomaly exists.

[0003] According to another implementation, a network device may be configured to receive one or more of user information, role information, or authorization information associated with a network access of a user, select a traffic flow to monitor that is associated with the one or more of user information, role information, or authorization information, store a traffic behavior pattern corresponding to the one or more of user information, role information, or authorization information, based on one or more previous network accesses by the user, compare traffic flow information, associated with the traffic flow, with information associated with the traffic behavior pattern, determine that an anomaly of traffic behavior exists when the traffic flow differs from the information associated with the traffic behavior pattern, and perform a security response when it is determined that the anomaly of traffic behavior exists.

[0004] According to still another implementation, a computer-readable medium may have stored thereon instructions, executable by at least one processor. The computer-readable medium may include one or more instructions for receiving one or more of user information, role information, or authorization information associated with a network access by a user, one or more instructions for selecting a traffic flow to monitor, where the traffic flow is associated with the network access, one or more instructions for monitoring the traffic flow, one or more instructions for determining whether an anomaly of traffic behavior exists with respect to the traffic flow by comparing the traffic flow with a traffic behavior pattern associated with the one or more of user information, role information, or authorization information, and one or more instructions for performing a security response when it is determined that the anomaly exists.

[0005] According to still another implementation, a network device may include means for receiving one or more of user information, role information, or authorization information associated with a granted network access to a user, means for selecting a traffic flow resulting from the granted network access, means for monitoring the selected traffic flow, means for receiving a traffic behavior pattern that is associated with the one or more of user information, role information, or authorization information, means for comparing information associated with the selected traffic flow with the traffic behavior pattern, means for determining whether an anomaly of traffic behavior exists based on the comparing, and means for providing a security response when it is determined that the anomaly of traffic behavior exists.

[0006] According to still another implementation, a device may be configured to receive traffic flow information, construct a traffic profile associated with one or more of user information, role information, or authorization information relating to a granted network access, update a traffic behavior pattern associated with the one or more of user information, role information, or authorization information based on the traffic profile, where the traffic behavior pattern includes values or ranges of values indicative of non-deviant traffic behavior, and provide the updated traffic behavior pattern to another device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate one or more embodiments described herein and, together with the description, explain these embodiments. In the drawings:

[0008] FIG. **1**A is a diagram illustrating an overview of exemplary embodiments described herein;

[0009] FIG. **1**B is a diagram illustrating an exemplary environment in which methods, devices, and systems described herein may be implemented;

[0010] FIG. **2** is a diagram illustrating exemplary components of the security device depicted in FIGS. **1**A and **1**B;

[0011] FIG. **3** is a diagram illustrating exemplary functional components of the security device depicted in FIGS. **1**A and **1**B;

[0012] FIG. **4**A is a diagram illustrating exemplary functional components of the database depicted in FIGS. **1**A and **1**B;

[0013] FIG. **4**B is a diagram of an exemplary traffic profile table;

[0014] FIG. **5**A is a flow diagram illustrating an exemplary process for detecting an anomaly of traffic behavior based on user information, role information, and/or authorization information;

[0015] FIG. **5**B is a flow diagram illustrating an exemplary process for creating and/or updating a traffic behavior pattern; and

[0016] FIGS. **6** and **7** are diagrams illustrating exemplary scenarios in which the embodiments described herein may be applied.

DETAILED DESCRIPTION

[0017] The following detailed description refers to the accompanying drawings. The same reference numbers in different drawings may identify the same or similar elements. Also, the following description does not limit the invention. Instead, the scope of the invention is defined by the appended claims and equivalents.

[0018] The term "user information," as used herein, is intended to be broadly interpreted to include, for example, a user's name, a string that includes a portion of the user's name, a user identifier (e.g., a string), or the like. The term "string," as used herein, is intended to be broadly interpreted to include (one or more of) letters, numbers, symbols, or some combination of letters, numbers, and/or symbols.

[0019] The term "role information," as used herein, is intended to be broadly interpreted to include, for example, a user's status, a user's role, a job title, an access level, or the like. A user may have more than one role.

[0020] The term "authorization information," as used herein, is intended to be broadly interpreted to include, for example, information that uniquely identifies a user and/or information that is provided by the user to access a network. While user information and/or role information may correspond to authorization information, authorization information may include information, other than user and/or role information. For example, authorization information may include password information, log-in information, authorization codes, credential information, and the like.

[0021] Embodiments described herein provide methods, devices, and systems that may utilize user information, role information, and/or authorization information to select and monitor traffic flows, and detect deviations or anomalies based on traffic behavior patterns associated with the user information, role information, and/or authorization information. It will be appreciated that use, role, and/or authorization information is typically not conveyed in a traffic flow or provided by, for example, a router or a switch. Thus, security devices that monitor traffic flows do not have this type of information. Accordingly, some techniques, which monitor traffic flows and detect deviations or anomalies, are based on content of traffic, source address, destination address, transport layer protocol, source port, and destination port. In an Internet Protocol-based network this information corresponds to a source (IP) address (SIP), destination IP address (DIP), transport layer protocol (PROT), source port (SPORT), and destination port (DPORT) (sometimes referred to as a 5-tuple (SIP, DIP, PRO, SPORT, DPORT)). Still, in other techniques, security devices that monitor traffic flows and detect deviations or anomalies are based on the 5-tuple information, as well as other information, such as, ingression interface, type of service (TOS), quality of service (QOS), timestamps, and number of packets/bytes of a traffic flow.

[0022] In one implementation, a security device may receive user, role, and/or authorization information associated with a network access request by a user and a network access grant. The security device may detect and monitor a traffic flow associated with the user, role and/or authorization information, resulting from the granted network access. Thereafter, the security device may recognize a deviation or an anomaly of traffic behavior by comparing the information associated with the monitored traffic flow to an existing traffic behavior pattern. In one implementation, the existing traffic behavior pattern may correspond to a history of traffic behavior associated with the user, role, and/or authorization information. In other implementations, the existing traffic behavior pattern may correspond to information created by a network administrator and considered normal or non-deviant. When the comparison reveals that a deviation or an anomaly exists, the security device may then provide an appropriate security response (e.g., closing the session, dropping packets, etc.) to the recognized deviation or anomaly. The security response may be user-configured.

[0023] FIG. **1**A is a diagram illustrating an overview of exemplary embodiments described herein. By way of example, user **105** may access a network with a user device **110**. User **105** may provide user, role and/or authentication information **115** to a device **120**. User **105** is authenticated and granted access to the network. Device **120** may share the user, role, and/or authentication information **130** with security device **125**. Device **120** may also provide security device **125** with, for example, source network address information. In other implementations, device **120** may provide security device **125** with other information (e.g., source port, destination network address, etc.), in addition to, or instead of, source network address information.

[0024] User **105** may access resource **140**. Security device **125** may utilize the source network address information, which is associated with the user, role, and/or authentication information **130**, to select traffic **135** as a traffic flow to monitor **145**.

[0025] Database **150** may store a traffic behavior pattern corresponding to the user, role, and/or authorization information. Security device **125** may send **155** the monitored traffic flow information to database **150**. Database **150** may update **160** the traffic behavior pattern with the received traffic flow and send **165** the updated traffic behavior pattern to security device **125**. Security device **125** may compare **170** the traffic behavior associated with traffic **135** with the updated traffic behavior pattern, both of which correspond to user, role, and/or authorization information **130**. Based on this comparison, security device **125** may determine whether an anomaly exists. Security device **125** may then take appropriate measures (e.g., a security response) when it is determined that an anomaly or a deviation from the traffic behavior pattern exists. On the other hand, if it is determined that an anomaly or a deviation does not exist, security device **125** may continue to monitor traffic **135**.

[0026] As an example, assume that user **105**, with an administrator role, normally utilizes file transfer protocol (FTP). However, in this session (i.e., traffic **135**), user **105**, in the administrator role, begins web surfing. In such an instance, security device **125** may recognize this as an anomaly by comparing the traffic behavior pattern with the traffic behavior associated with traffic **135**. Security device **125** may then take appropriate security measures.

[0027] Since the embodiments have been broadly described, variations exist. Accordingly, a detailed description of the embodiments is provided below.

Exemplary Environment

[0028] FIG. **1**B is a diagram illustrating an exemplary environment **100** in which methods, devices, and systems described herein may be implemented. As illustrated in FIG. **1**B, environment **100** may include user **105** and user device **110** communicatively coupled to a network **115**. Network **115** may include an access device **120**, security device **125**, resources **140-1** and **140-2** (referred to generally as "resource **140**"), and database **150**. User **105**, user device **110**, access device **120**, security device **125**, resource **140**, and database **150**, depicted in FIG. **1**B, may correspond to user **105**, user device **110**, device **120**, security device **125**, resource **140**, and database **150** respectively, as previously illustrated and described with respect to FIG. **1**A.

[0029] The number of devices and configuration in environment **100** is exemplary and provided for simplicity. In practice, environment **100** may include more, fewer, different, and/or differently arranged devices than those illustrated in FIG. **1**. Also, some functions described as being performed by a particular device may be performed by a different device or a combination of devices. For example, in other embodiments, the functions associated with database **150** may be incorporated into security device **125**. Environment **100** may include wired and/or wireless connections among the devices.

[0030] User device **110** may include a device having the capability to communicate with other devices, systems, networks, and/or the like. For example, user device **110** may correspond to a computer (e.g., a laptop, a desktop, a handheld computer), a personal digital assistant, a wireless telephone, an Internet-browsing device, or another type of communication device.

[0031] Network **115** may include one or multiple networks of any type. For example, network **115** may include a private network, a public network, a local area network (LAN), a metropolitan area network (MAN), a wide area network (WAN), the Internet, an intranet, a telephone network (e.g., the Public Switched Telephone Network (PSTN) or a cellular network), a satellite network, a computer network, and/or a combination of networks.

[0032] Access device **120** may include a device having the capability to communicate with other devices, systems, networks, and/or the like. For example, access device **120** may include an application authentication server, a policy server, an enforcement point, and/or some other type of access control device or a device (e.g., a switch, a gateway, a bridge) that may process and/or forward network traffic. Access device **120** may be enabled at layer **2**, layer **3**, and/or at higher layers. Access device **120** may manage access to network **115**, including insider threats, guest user access, regulatory compliance, off-shoring and/or outsourcing. Access device **120** may obtain user information, role information, and/or authentication information, as well as other types of information, such as, for example, user device security state information, and/or location data. Access device **120** may define dynamic access control policies that are distributed within network **115**. In some implementations, access device **120** may provide pre-authentication assessments, role mapping, and resource controls. Access device **120** may support various standards, such as Institute of Electrical and Electronics Engineers (IEEE 802.1X), Remote Authentication Dial In User Service (RADIUS), Internet Protocol Security (IPsec), or the like.

[0033] Security device **125** may include a device having the capability to communicate with other devices, systems, networks, and/or the like. For example, security device **125** may include a security device (e.g., an IDP device). Security device **125** may also behave as some other type of device (e.g., a router, a switch, or the like) that may process and/or forward network traffic. Security device **125** may operate in an in-line mode and/or in a passive mode. Security device **125** may monitor and/or collect network and application data with respect to other devices (e.g., user device **110**, access device **120**, resource **140**) in network **115**.

[0034] Security device **125** may provide various security measures, such as, for example, stateful signature detection (i.e., signature-based detection), protocol anomaly detection (e.g., protocol usage against published Request For Comments (RFCs)), traffic anomaly detection (e.g., heuristic rules may detect traffic patterns that suggest reconnaissance or attacks), response to denial of service (DOS) attacks, Internet Protocol (IP) spoofing detection, and/or layer **2** attack detection. Security device **125** may support various active responses to an attack or threat detected, such as for example, dropping a packet, closing a connection, closing a client, closing a server, closing both a client and a server, and the like, as well as passive responses, such as, for example, logging information and a transport control protocol (TCP) reset.

[0035] Security device **125** may provide other types of services, such as, for example, role-based administration and/or domain-based administration (e.g., to enable a logical separation of devices, policies, reports, etc.). Security device **125** may also provide logging (e.g., collecting network traffic information, traffic pattern information, etc.), and reporting/notification (e.g., providing real-time reports). In one embodiment, security device **125** may include a profiler. The profiler may capture accurate and granular details associated with a traffic flow. An exemplary profiler is described in greater detail below.

[0036] Resource **140** may include a device that provides a service, data, and/or some other type of asset. For example, resource **140** may correspond to a Web server, a mail server, a data repository, or the like.

[0037] Database **150** may store and manage traffic profile information and traffic behavior pattern information. Database **150** may analyze and create traffic profiles based on traffic flow information received from security device **125**. Database **150** may also update traffic behavior pattern information with traffic profile information.

[0038] While security device **125** may be implemented as different types of devices, in the following paragraphs, security device **125** will be described in terms of an IDP device.

Exemplary Device Architecture

[0039] FIG. **2** is a diagram illustrating exemplary components of security device **125**. As illustrated, security device **115** may include, for example, a bus **210**, a processor **220**, a memory **230**, storage **240**, an input/output **250**, and a communication interface **260**.

[0040] Bus **210** may permit communication among the other components of security device **125**. For example, bus **210** may include a system bus, an address bus, a data bus, and/or a control bus. Bus **210** may also include bus drivers, bus arbiters, bus interfaces, and/or clocks.

[0041] Processor **220** may interpret and/or execute instructions and/or data. For example, processor **220** may include a processor, a microprocessor, a data processor, a co-processor, a network processor, an application specific integrated circuit (ASIC), a controller, a programmable logic device, a field programmable gate array (FPGA), or some other processing logic that may interpret and/or execute instructions.

[0042] Memory **230** may store data and/or instructions. For example, memory **230** may include a random access memory (RAM), a dynamic random access memory (DRAM), a static random access memory (SRAM), a synchronous dynamic random access memory (SDRAM), a read only memory (ROM), a programmable read only memory (PROM), an erasable programmable read only memory (EPROM), an electrically erasable programmable read only memory (EEPROM), another type of dynamic or static memory, a cache, and/or a flash memory.

[0043] Storage **240** may store data, instructions, and/or applications. For example, storage **240** may include a hard disk (e.g., a magnetic disk, an optical disk, a magneto-optic disk, etc.), a compact disc (CD), a digital versatile disc (DVD), a floppy disk, a cartridge, a magnetic tape, a flash drive, or another type of computer-readable medium, along with a corresponding drive. The term "computer-readable medium" is intended to be broadly interpreted to include, for example, memory, storage or the like. A computer-readable medium may be implemented in a single device, in multiple devices, in a centralized manner, or in a distributed manner.

[0044] Input/output **250** may permit input to and output from security device **115**. For example, input/output **250** may include a keyboard, a keypad, a mouse, a button, a switch, a microphone, voice recognition logic, a pen, a display, a port, or the like to permit input. Additionally, or alternatively, input/output **250** may include a display, a speaker, one or more light emitting diodes (LEDs), a port, or the like, to permit output.

[0045] Communication interface **260** may enable security device **125** to communicate with another device, a network, another system, and/or the like. For example, communication interface **260** may include a wireless interface and/or a wired interface, such as, an Ethernet interface, an optical interface, etc. Communication interface **260** may include a transceiver.

[0046] Security device **125** may perform operations and/or processes related to defining and analyzing traffic behavior patterns based on user, role, and/or authorization information, and to detecting deviations or anomalies associated with these traffic behavior patterns. According to an exemplary implementation, security device **125** may perform these operations and/or processes in response to processor **220** executing sequences of instructions contained in a computer-readable medium. For example, software instructions may be read into memory **230** from another computer-readable medium, such as storage **240**, or from another device via communication interface **260**. The software instructions contained in memory **230** may cause processor **220** to perform processes that will be described later. Alternatively, hardwired circuitry may be used in place of or in combination with software instructions to implement processes described herein. Thus, implementations described herein are not limited to any specific combination of hardware circuitry and software.

[0047] Although, FIG. **2** illustrates exemplary components of security device **125**, in other implementations, security device **125** may include additional, fewer, different, or differently arranged components than those illustrated in FIG. **2** and described herein. Additionally, or alternatively, one or more operations described as being performed by a particular component of security device **125** may be performed by one or more other components, in addition to or instead of the particular component. Additionally, it will be appreciated that other devices (e.g., user device **110**, access device **120**, resource **140**, and/or database **150**) in environment **100** may include the exemplary components illustrated in FIG. **2**.

[0048] FIG. **3** is a diagram of exemplary functional components of security device **125**. As illustrated in FIG. **3**, security device **125** may include a detection engine **305**, a database **310**, and a profiler **315**. The functional components illustrated in FIG. **3** may be implemented by hardware (e.g., processor **220**) or a combination of hardware and software. While a particular number and arrangement of components are illustrated in FIG. **3**, in other implementations, security device **125** may include fewer, additional, different, or differently arranged components than those illustrated in FIG. **3**. Further, it will be appreciated that these functional components may be implemented in other devices (e.g., user device **110**, access device **120**, resource **140**, and/or database **150**) in environment **100**.

[0049] Detection engine **305** may receive network traffic in the form of packets. While packets will be used in the description herein, implementations described herein apply to any form of a data unit, either in the form of a packet, a non-packet, a cell, a datagram, bits, bytes, etc. Detection engine **305** may perform various detection methods, such as, for example, pattern matching, signature matching, stateful pattern matching, and/or anomaly-based detection (e.g., protocol, traffic), necessary to identify attacks, threats, and/or malicious traffic.

[0050] Database **310** may store various types of information relating to the operation of security device **125**. For example, database **310** may store signatures and/or heuristics for identifying anomalies, threats, attacks, and/or malicious traffic. Database **310** may store protocol decode information and policies.

[0051] Profiler **315** (or detection engine **305**) may detect, monitor, and analyze traffic patterns. For example, profiler **315** may detect and monitor traffic that traverses network **115**. Profiler **315** (or detection engine **305**) may also compare a traffic behavior pattern with traffic flow information to determine whether an anomaly of traffic behavior exists. As described herein, in one implementation, profiler **315** may retrieve or receive a traffic behavior pattern from database **150**. When it is determined that an anomaly exists, security device **125** may take appropriate security measures.

[0052] FIG. **4**A is a diagram illustrating exemplary functional components of the database depicted in FIGS. **1**A and **1**B. The functional components illustrated in FIG. **4**A may be implemented by hardware (e.g., processor **220**) or a combination of hardware and software. While a particular number and arrangement of components are illustrated in FIG. **4**A, in other implementations, database **150** may include fewer, additional, different, or differently arranged components than those illustrated in FIG. **4**A. Further, it will be appreciated that these functional components may be implemented in other devices (e.g., user device **110**, access device **120**, security device **125**, and/or resource **140**) in environment **100**.

[0053] Network traffic analyzer **405** may create a traffic profile based on the monitored traffic associated with a particular user, role, and/or authorization information. In one implementation, security device **125** may provide database **150** (e.g., network traffic analyzer **405**) with the monitored traffic flow information. In other implementations, network traffic analyzer **405** may retrieve traffic flow information from security device **125**. FIG. **4**B is a diagram of an exemplary traffic profile table.

[0054] As illustrated in FIG. **4**B, traffic profile table **415** may include a user information field **420**, a role information field **425**, an authorization information field **430**, and a traffic behavior pattern information field **435**. The information fields of traffic profile table **415** may be arranged according to an individual basis, a group basis, a domain basis, or the like.

[0055] User information field **420** may include user information. By way of example, user information field **420** may include a user's name (e.g., Kevin Smith), a string that identifies a user (e.g., TWT12598), or some other type of information (User name=Visitor).

[0056] Role information field **425** may include role information. By way of example, role information field **425** may include a user status (e.g., Employee), a job title (e.g., Administrator), or an access level (e.g., Guest).

[0057] Authorization information field **430** may include authorization information. By way of example, authorization information field **430** may include password information, log-in information, authorization codes, credential information, or the like.

[0058] Traffic behavior pattern information field **435** may include source address, destination address, source port, destination port, and transport protocol information (e.g., 5-tuple information (SIP, DIP, PRO, SPORT, DPORT)) and content information, which is typically conveyed in a traffic flow, as well as other information, such as, for example, ingression interface, TOS, QOS, timestamps, and number of packets/bytes of a traffic flow. This type of information may be utilized to create a traffic behavior pattern that may be associated with user, role, and/or authorization information. For example, the number of packets/bytes of a traffic flow may be used to formulate a traffic volume of use per session or over a period of time. In another example, the type of service information may be used to formulate a history of services normally utilized or accessed by a user, a role, and associated authorization information. In still another example, a source address and/or a destination address may be used to formulate a history regarding the user device that the user, the role, and/or the corresponding authorization information normally uses to access the network, or which destination devices the user, the role, and/or the corresponding authorization information normally accesses or utilizes. Thus, in general, traffic information captured by security device **125** (e.g., profiler **315**) may be used to construct the traffic behavior pattern and associate this with user, role, and/or authorization information.

[0059] Although FIG. **4**B illustrates an exemplary traffic profile table **415**, in other implementations, traffic profile table **415** may include additional, different, or few information fields than illustrated in FIG. **4**A and described herein.

[0060] Referring back to FIG. **4**A, network traffic analyzer **405** may create a traffic behavior pattern based on traffic profile information associated with a particular user, role, and/or authorization information. Network traffic analyzer **405** may store the created traffic behavior pattern in database **410**. Network traffic analyzer **405** may utilize various techniques to create the traffic behavior pattern, such as, for example, statistical analysis, averaging, etc., with respect to traffic flow information, such as, for example, content information, source address, source port, destination address, destination port, transport protocol (e.g., 5-tuple information), ingression interface, TOS, QOS, timestamps, and number of packets/bytes associated with traffic flow. The number of sessions needed to establish and/or create the traffic behavior pattern may be user-configurable. A traffic behavior pattern table may correspond to traffic profile table **415**, however, the traffic behavior pattern table may include values or a range of values associated with traffic behavior pattern information **435** that are representative of normal traffic pattern behavior.

[0061] In an alternative implementation, the traffic behavior pattern may be created by, for example, an administrator or some other network personnel. For example, the administrator may determine values or a range of values that are considered normal or representative of non-deviant traffic behavior, and create a traffic behavior pattern table. The administrator may associate the traffic behavior pattern to a particular user, group of users, role(s), and/or authorization information. In either implementation, the traffic behavior pattern may equate to normal traffic behavior, which may be used to detect abnormal traffic behavior. It will be appreciated, that the term "traffic behavior pattern," as used herein, may correspond to a traffic behavior pattern created by database **150** (e.g., network traffic analyzer **405**), a traffic behavior pattern created by, for example, a network administrator, and/or a combination of both.

[0062] Once the traffic behavior pattern is created, network traffic analyzer **405** may update the traffic behavior pattern with subsequent sessions (e.g., monitored traffic flows) associated with the particular user, role, and/or authorization information. For example, network traffic analyzer **405** may create a traffic profile based on the monitored traffic flow. Network traffic analyzer **405** may then update the traffic behavior pattern based on the traffic profile.

Exemplary Process

[0063] As described herein, security device **125** may utilize user, role, and/or authorization information to select and monitor traffic flows, and detect deviations or anomalies based on traffic behavior patterns associated with the user information, role information, and/or authorization information. It is recognized, that although, the description provides that user, role, and/or authorization information may be obtained by a device (e.g., device **120** or access device **120**) and forwarded to security device **125**, in other implementations, this functionality may be implemented within a single device. That is, security device **125** may obtain the user, role, and/or authorization information.

[0064] FIG. **5**A is a flow diagram illustrating an exemplary process **500** for selecting and monitoring traffic flows, and detecting deviations or anomalies based on traffic behavior patterns associated with user information, role information, and/or authorization information. Process **500** may be performed by hardware (e.g., processor **220** and/or some other type of logic), or a combination of hardware and software in security device **125**. In another implementation, one or more operations associated with process **500** may be performed by another device in conjunction with security device **125**. Process **500** will be described in conjunction with other figures. For purposes of discussion, it will be assumed that a traffic behavior pattern exists in database **150**. This is in contrast in which an initial state of database **150** requires that the traffic behavior pattern be created versus updated.

[0065] Process **500** may begin with receiving user, role, and/or authorization information (block **505**). For example, as illustrated in FIG. **1**B, user **105** may attempt to access network **115**. User **105** may be required to provide information to access device **120** before access is granted. This information may include user, role, and/or authorization information. Access device **120** may also obtain other types of information based on communication with user device **110**, such as, for example, source network address, source port, destination network address, destination port, protocol (e.g., transport level), as well as other information, such as, for example, ingression interface, type of service (TOS), quality of service (QOS), timestamps, and number of packets/bytes of a traffic flow. For purposes of discussion, assume that access device **120** grants user **105** access to network **115**.

[0066] Returning to FIG. **5**A, user, role, and/or authorization information may be forwarded to the security device

(block **510**). Access device **120** may forward the received user, role, and/or authorization information to security device **125**. Security device **125** may store the user, role, and/or authorization information in traffic behavior table **400** of database **310**. Access device **120** may forward other information (e.g., source network address, source port, etc.) to security device **125**. Security device **125** may also store this information in traffic behavior table **400**.

[0067] Network traffic based on user, role, and/or authorization information may be monitored (block **515**). Security device **125** (e.g., profiler **315**) may detect, select, and/or monitor traffic from user **105** based on the user, role, and/or authorization information. For example, as illustrated in FIG. **1**A, security device **125** may monitor traffic **135** associated with user **105** and user device **110**. In one implementation, security device **125** may identify which traffic belongs to user **105** based on source network address, source port, etc., and/or the user, role, and/or authorization information provided by access device **120**. Additionally, or alternatively, security device **125** may utilize information contained in traffic **135** to associate the user, role, and/or authorization information with traffic **135**.

[0068] The monitored network traffic flow may be provided to update a traffic behavior pattern (block **520**). Security device **125** may provide the monitored traffic flow to database **150**. The monitored traffic flow may include the traffic flow information as well as user, role, and/or authorization information. In one implementation, security device **125** may transmit the monitored traffic flow to database **150**. In other implementations, database **150** may retrieve the monitored traffic flow.

[0069] An updated traffic behavior pattern may be obtained (block **525**). Security device **125** may obtain the updated traffic behavior pattern from database **150**. The updated traffic behavior pattern may include information representative of normal traffic behavior associated with the user, role, and/or authorization information. In one implementation, security device **125** may retrieve the updated traffic behavior pattern from database **150**. In other implementations, database **150** may transmit the updated traffic behavior pattern to security device **125**.

[0070] It may be determined whether an anomaly exists between the traffic behavior pattern and the traffic behavior (i.e., corresponding to a current session). For example, profiler **315** may compare the traffic behavior pattern with the traffic behavior corresponding to the current session to determine whether an anomaly of traffic behavior exists.

[0071] In some implementations, profiler **315** may create a traffic behavior profile based on the traffic behavior corresponding to the current session, before a comparison between the traffic behavior pattern and the traffic behavior corresponding to the current session is made. In other implementations, profiler **315** may perform a comparison without further processing of the monitored traffic flow.

[0072] Profiler **315** may detect an anomaly based on the comparison. That is, the comparison may reveal that the traffic behavior associated with the monitored traffic flow deviates from "normal" behavior represented by the traffic behavior pattern for this particular user, role, and/or authorization information. By way of example, an anomaly could correspond to user **105** accessing network **115** from a different source address, user **105** utilizing a different service, user **105** exceeding a number of bytes uploaded and/or downloaded, etc.

[0073] As illustrated in FIG. **5**A, if it is determined that an anomaly exists (block **530**-YES), security device **125** may perform one or more appropriate security measures (block **535**). These security measure(s) may be user-configurable. For example, security device **125** may consult database **310** to identify the appropriate security measures. As previously mentioned, security response may include closing the session, dropping packets, logging information, closing a client, closing a server, closing both the client and the server, etc. In one implementation, one or more security measures may be mapped based on the user, role, and/or authorization information. That is, the security policies of network **115** may be mapped to the user, role, and/or authorization information. Additionally, or alternatively, the security policies of network **115** may mapped to source address, source port, etc., associated with the monitored traffic flow.

[0074] On the other hand, if it is determined that an anomaly does not exist (block **530**-NO), security device **125** may continue to monitor the network traffic flow (block **540**). That is, security device **125** may continue to monitor the network traffic flow associated with the current session.

[0075] Although FIG. **5**A illustrates an exemplary process **500**, in other implementations, fewer, additional, or different operations may be performed.

[0076] FIG. **5**B is a flow diagram illustrating an exemplary process **550** for creating and/or updating a traffic behavior pattern. Process **550** may be performed by hardware (e.g., processor **220** and/or some other type of logic), or a combination of hardware and software in database **150**. In another implementation, one or more operations associated with process **550** may be performed by another device (e.g., security device **125**) in conjunction with database **150**. Process **550** will be described in conjunction with other figures.

[0077] Process **550** may begin by obtaining network traffic flow information (block **555**). Database **150** may obtain monitored traffic flow information. The monitored traffic flow information may include information associated with traffic **135** as well as user, role, and/or authorization information. In one implementation, database **150** may retrieve the monitored traffic flow information from security device **125**. In other implementations, security device **125** may transmit the monitored traffic flow information to database **150**.

[0078] A traffic flow profile may be created (block **560**). Database **150** (e.g., network traffic analyzer **405** may create a traffic profile (e.g., traffic profile table) based on the monitored traffic flow information. For example, network traffic analyzer **405** may analyze the monitored traffic flow information to create the traffic profile.

[0079] It may be determined whether a traffic behavior pattern exists (block **565**). For example, network traffic analyzer **405** may consult database **410** to determine whether a traffic behavior pattern exists with respect to the user, role, and/or authorization. In practice, a traffic behavior pattern may be created within a user-configured time period (e.g., a day, a week, a month, etc.). However, the number of sessions in which network traffic analyzer **405** considers sufficient to create a traffic behavior pattern, or considers that a traffic behavior pattern exists, may be a user-configurable parameter. It will be appreciated that the traffic behavior pattern may be created by, for example, a network administrator, as previously described. In this instance, block **565** may be omitted.

[0080] If it is determined that a traffic behavior pattern does not exist (block **565**-NO), then network traffic analyzer **405** may create a traffic behavior pattern based on the traffic

profile (block **570**). The traffic behavior pattern may be associated with the user, role, and/or authorization information. Depending on the number of sessions and corresponding traffic behavior, network traffic analyzer **405** may utilize various techniques to create the traffic behavior pattern, such as, for example, statistical analysis, averaging, etc. The traffic behavior pattern may include values, range of values, parameters, etc. relating to traffic flow that represent or are indicative of normal traffic behavior.

[0081] If it is determined that the traffic behavior pattern does exist (block **565**-YES), then network traffic analyzer **405** may update the traffic behavior pattern based on the traffic profile (block **575**). For example, network traffic analyzer **405** may utilize the information associated with the traffic profile to update values, range of values, parameters, etc. relating to traffic flow.

[0082] The updated traffic behavior pattern may be provided (block **580**). Database **150** (e.g., network traffic analyzer **405**) may transmit the updated traffic behavior pattern to security device **125**. In other implementation, security device **125** may retrieve the updated traffic behavior pattern (e.g., an updated traffic behavior pattern table) from database **410**.

[0083] Although FIG. **5**B illustrates an exemplary process **550**, in other implementations, fewer, additional, or different operations may be performed.

EXAMPLES

[0084] FIGS. **6** and **7** are diagrams illustrating examples of detecting, selecting and monitoring traffic flows, and detecting deviations or anomalies based on traffic behavior patterns associated with the user information, role information, and/or authorization information. Based on the detected deviations or anomalies, security device **125** may provide a finer granularity of security protection.

[0085] For example, as illustrated in FIG. **6**, user **105-1** may have a role of an administrator, user **105-2** may have a role of a developer, and user **105-3** may have a role of an employee. Assume that users **105** access resource **140-1** or **140-2** at different times. Also, assume that user device **110** utilizes (or is assigned) the same source address (e.g., a same IP address) each time. As illustrated, each user **105** may provide user, role, and/or authorization information to access device **120**. Access device **120** may forward the received user, role, and/or authorization information to security device **125**. Access device **120** may also forward the same source address to security device **125**. Security device **125** may detect, select, and monitor the traffic and determine whether an anomaly exists, as previously described. Unlike existing techniques, which may view the traffic as coming from the same source (i.e., source address), and may require a deeper level of traffic inspection (e.g., 5-tuple level), security device **125** may provide a finer granularity of security with respect to the traffic since user, role, and/or authorization information is utilized. As a result, security device **125** may provide for appropriate security measures in response to detected deviations or anomalies of traffic behavior that may exist in such a scenario.

[0086] In another example, as illustrated in FIG. **7**, a single user **105** may access resources **140-1** or **140-2**, at different times, on different user devices **110** (i.e., user device **110-1**, **110-2**, and **110-3**) with different role information (e.g., Administrator, Developer, and Employee). That is, user **105** may have three different roles. User devices **110-1**, **110-2**, and **110-3** may utilize (or be assigned) different source addresses (e.g., an IP address **1**, an IP address **2**, and an IP address **3**). Access device **120** may forward the received user, role, and/or authorization information to security device **125**. Access device **120** may also forward the different source addresses. Security device **125** may detect, select, and monitor the traffic and determine whether an anomaly exists, as previously described. Unlike existing techniques, which may view the separate traffic as coming from different sources, since the source addresses are different, and may correspondingly apply different security policies, security device **125** may provide a finer granularity of security with respect to the traffic since user, role, and/or authorization information is utilized. As a result, security device **125** may provide for appropriate security measures in response to detected deviations or anomalies of traffic behavior that may exist in such a scenario.

CONCLUSION

[0087] The foregoing description of implementations provides an illustration, but is not intended to be exhaustive or to limit the implementations to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practice of the teachings. For example, security device **125** and database **150** may be implemented on a single device. Additionally, or alternatively, security device **125** may store a traffic behavior pattern in database **310**. Additionally, or alternatively, once a traffic behavior pattern is created it may not be updated based on a traffic profile. For example, security device **125** may compare the monitored traffic flow with a stored traffic behavior pattern in database **310**, without updating the traffic behavior pattern. Additionally, or alternatively, updates to the traffic behavior pattern may be performed by, for example, a network administrator, in addition to, or instead of traffic profile information. Additionally, or alternatively, a traffic behavior pattern may be updated with the monitored traffic flow only after security device **125** determines that the traffic behavior associated the monitored traffic flow is indicative of normal or non-anomalies traffic behavior. In this implementation, database **150** may not update the traffic behavior pattern with the monitored traffic flow before this determination is made.

[0088] In addition, while a series of blocks has been described with regard to the processes illustrated in FIG. **5**A and FIG. **5**B, the order of the blocks may be modified in other implementations. Further, non-dependent blocks may be performed in parallel.

[0089] Also, certain aspects have been described as being implemented as "logic" or a "component" that performs one or more functions. This logic or component may include hardware, such as a processor, microprocessor, an ASIC, or a FPGA, or a combination of hardware and software, such as a processor/microprocessor executing instructions stored in a computer-readable medium.

[0090] It will be apparent that aspects described herein may be implemented in many different forms of software, firmware, and hardware in the implementations illustrated in the figures. The actual software code or specialized control hardware used to implement aspects does not limit the embodiments. Thus, the operation and behavior of the aspects were described without reference to the specific software code—it being understood that software and control hardware can be designed to implement the aspects based on the description herein.

[0091] The term "may" is used throughout this application and is intended to be interpreted, for example, as "having the

potential to," "configured to," or "being able," and not in a mandatory sense (e.g., as "must"). The terms "a," "an," and "the" are intended to be interpreted to include one or more items. For example, a processor **302** may include one or more processors. Where only one item is intended, the term "one" or similar language is used. Further, the phrase "based on" is intended to be interpreted as "based, at least in part, on," unless explicitly stated otherwise. The term "and/or" is intended to be interpreted to include any and all combinations of one or more of the associated list items.

[0092] Even though particular combination of features are recited in the claims and/or disclosed in the specification, these combinations are not intended to limit the disclosure of the invention. In fact, many of these features may be combined in ways not specifically recited in the claims and/or disclosed in the specification.

[0093] No element, block, or instruction used in the present application should be construed as critical or essential to the implementations described herein unless explicitly described as such.

What is claimed is:

1. A method performed by a device, comprising:
receiving, by the device, one or more of user information, role information, or authorization information associated with a user accessing a network;
selecting, by the device, a traffic flow to monitor that is associated with the one or more of user information, role information, or authorization information;
monitoring, by the device, the traffic flow;
determining, by the device, whether an anomaly of traffic behavior exists with respect to the traffic flow based on a traffic behavior pattern associated with the one or more of user information, role information, or authorization information; and
performing, by the device, a security response when it is determined that the anomaly exists.

2. The method of claim **1**, where the determining comprises:
comparing, by the device, the traffic behavior pattern history with traffic behavior corresponding to the traffic flow; and
determining, by the device, whether the anomaly exists based on the comparing.

3. The method of claim **2**, further comprising:
receiving, by the device, the traffic behavior pattern, from another device.

4. The method of claim **1**, where the user information includes one of the user's name, a string that includes a portion of the user's name, or a string that corresponds to the user.

5. The method of claim **1**, where the role information includes one of the user's status, a job title, or the user's access level.

6. The method of claim **1**, where the authorization information includes one of password information, log-in information, authorization code, or credential information.

7. The method of claim **1**, where the receiving comprises:
receiving, by the device, the one or more of user information, role information, or authorization information from a user device utilized by the user to access the network, or
receiving, by the device, the one or more of user information, role information, or authorization information from another device that regulates network access by the user.

8. The method of claim **1**, further comprising:
storing, by the device, security policies; and
where the performing comprises:
selecting, by the device, one of the security policies corresponding to the anomaly, when it is determined that the anomaly exists; and
performing, by the device, the security response corresponding to the one of the security policies.

9. A network device, to:
receive one or more of user information, role information, or authorization information associated with a network access of a user;
select a traffic flow to monitor that is associated with the one or more of user information, role information, or authorization information;
store a traffic behavior pattern corresponding to the one or more of user information, role information, or authorization information, based on one or more previous network accesses by the user;
compare traffic flow information, associated with the traffic flow, with information associated with the traffic behavior pattern;
determine that an anomaly of traffic behavior exists when the traffic flow differs from the information associated with the traffic behavior pattern; and
perform a security response when it is determined that the anomaly of traffic behavior exists.

10. The network device of claim **9**, where the network device is further configured to:
receive the traffic behavior pattern from another device.

11. The network device of claim **9**, where the network device includes an intrusion, detection, and prevention device.

12. The network device of claim **9**, where the network device is further configured to:
continue to monitor the traffic flow, when it is determined that the anomaly does not exist.

13. The network device of claim **9**, where the traffic flow information includes one or more of source address, source port, destination address, destination port, protocol, type of service, quality of service, timestamp information, or number of packets or bytes.

14. The network device of claim **9**, where the network device is further configured to:
monitor the traffic flow; and
obtain the traffic flow information from the traffic flow monitored.

15. The network device of claim **9**, where the network device is further configured to receive a source address or a source port associated with the network access of the user, and where, when selecting the traffic flow, the network device is further configured to:
select the traffic flow to monitor based on the source address or the source port, which is associated with the one or more of user information, role information, or authorization information.

16. A computer-readable medium having stored thereon instructions, executable by at least one processor, the computer-readable medium comprising:
one or more instructions for receiving one or more of user information, role information, or authorization information associated with a network access by a user;
one or more instructions for selecting a traffic flow, where the traffic flow is associated with the network access;

one or more instructions for monitoring the traffic flow;

one or more instructions for determining whether an anomaly of traffic behavior exists with respect to the traffic flow by comparing the traffic flow with a traffic behavior pattern associated with the one or more of user information, role information, or authorization information; and

one or more instructions for performing a security response when it is determined that the anomaly exists.

17. The computer-readable medium of claim **16**, where the traffic behavior pattern is based on one or more previous monitorings of traffic flows associated with the one or more of user information, role information, or authorization information.

18. The computer-readable medium of claim **16**, further comprising:

one or more instructions for updating the traffic behavior pattern history based on information associated with the traffic flow, when it is determined that the anomaly does not exist.

19. A network device, comprising:

means for receiving one or more of user information, role information, or authorization information associated with a granted network access to a user;

means for selecting a traffic flow resulting from the granted network access;

means for monitoring the selected traffic flow;

means for receiving a traffic behavior pattern associated with the one or more of user information, role information, or authorization information;

means for comparing information associated with the selected traffic flow with the traffic behavior pattern;

means for determining whether an anomaly of traffic behavior exists based on the comparing; and

means for providing a security response when it is determined that the anomaly of traffic behavior exists.

20. A device, to:

receive traffic flow information;

construct a traffic profile associated with one or more of user information, role information, or authorization information relating to a granted network access;

update a traffic behavior pattern associated with the one or more of user information, role information, or authorization information based on the traffic profile, where the traffic behavior pattern includes values or ranges of values indicative of non-deviant traffic behavior; and

provide the updated traffic behavior pattern to another device.

* * * * *