

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214425 A1 Ossipov et al.

(43) **Pub. Date:**

Jun. 27, 2024

(54) USING AN END-TO-END POLICY CONTROLLER TO AUTOMATICALLY DISCOVER AND INVENTORY ENFORCEMENT POINTS IN A NETWORK (52) U.S. Cl. CPC H04L 63/20 (2013.01); G06F 9/451 (2018.02); **H04L 63/105** (2013.01)

(71) Applicant: Cisco Technology, Inc., San Jose, CA

(57)ABSTRACT

(72) Inventors: Andrew E. Ossipov, Lewisville, TX (US): Janardhanan Radhakrishnan. Dublin, CA (US); Robert Tappenden, South Melbourne (AU); Jared Tierney Smith, Liberty Hill, TX (US)

(21) Appl. No.: 18/089,252 Filed: Dec. 27, 2022

Publication Classification

(51) **Int. Cl.** H04L 9/40 (2006.01)G06F 9/451 (2006.01)

Techniques for using an end-to-end policy controller to automatically discover and inventory enforcement points in a network. A network controller may leverage data associated with network devices in a network to identify paths between source endpoints and destination endpoints to establish an inventory of enforcement points along the paths. For example, the controller may consume telemetry data indicative of network events (e.g., firewall events, IPS event logs, netflow events, etc.) to figure out where enforcement points are provisioned with respect to traffic being observed. Additionally, the SDN controller may dynamically build a network topology providing indications of roles and/or locations of enforcement points.

500 -

RECEIVE DATA REPRESENTING AN INTENT-BASED SECURITY POLICY ASSOCIATED WITH A NETWORK, THE INTENT-BASED SECURITY POLICY INDICATING AN ENTITY, A RESOURCE, AND AN AUTHORIZATION ASSOCIATED WITH THE ENTITY ACCESSING THE RESOURCE

502

DETERMINE A PATH OF NETWORK TRAFFIC BETWEEN THE ENTITY AND THE RESOURCE BASED AT LEAST IN PART ON THE AUTHORIZATION. THE PATH OF NETWORK TRAFFIC INCLUDING ONE OR MORE NETWORK DEVICES 504

IDENTIFY, BY A SOFTWARE-DEFINED NETWORKING (SDN) CONTROLLER ASSOCIATED WITH THE NETWORK AND BASED AT LEAST IN PART ON AN INVENTORY STORING INFORMATION ASSOCIATED WITH THE NETWORK DEVICES, ONE OR MORE ENFORCEMENT POINTS ASSOCIATED WITH THE PATH OF NETWORK TRAFFIC

506

DETERMINE THAT A FIRST ENFORCEMENT POINT OF THE ONE OR MORE ENFORCEMENT POINTS ASSOCIATED WITH THE PATH OF NETWORK TRAFFIC HAS A FIRST CAPABILITY TO IMPLEMENT AT LEAST A FIRST PORTION OF THE INTENT-BASED SECURITY POLICY

<u>508</u>

DETERMINE THAT A SECOND ENFORCEMENT POINT OF THE ONE OR MORE ENFORCEMENT POINTS ASSOCIATED WITH THE PATH OF NETWORK TRAFFIC HAS A SECOND CAPABILITY TO IMPLEMENT AT LEAST A SECOND PORTION OF THE INTENT-BASED SECURITY POLICY

510

GENERATE A FIRST CHAIN OF ENFORCEMENT POINTS BASED AT LEAST IN PART ON THE FIRST ENFORCEMENT POINT AND THE SECOND ENFORCEMENT POINT 512

SEND THE FIRST PORTION OF THE INTENT-BASED POLICY AND THE SECOND PORTION OF THE INTENT-BASED POLICY TO THE FIRST CHAIN OF ENFORCEMENT POINTS 514