

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214424 A1 Ossipov et al.

(43) **Pub. Date:**

Jun. 27, 2024

(54) USING AN END-TO-END POLICY CONTROLLER TO SPLIT POLICIES BETWEEN ENFORCEMENT POINTS IN A **NETWORK**

(52) U.S. Cl. CPC *H04L 63/20* (2013.01)

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

(72) Inventors: Andrew E. Ossipov, Lewisville, TX

(US); Robert Tappenden, South Melbourne (AU); Janardhanan Radhakrishnan, Dublin, CA (US); Chandrodaya Prasad, San Jose, CA (US)

(21) Appl. No.: 18/089,212

(22) Filed: Dec. 27, 2022

Publication Classification

(51) Int. Cl. H04L 9/40

(2006.01)

(57)ABSTRACT

Techniques for using an end-to-end policy controller to utilize an inventory of enforcement points to generate a chain of enforcement points having capabilities to enforcement individual operations of an intent-based security policy associated with an entity accessing a resource. A network controller may intelligently split an intent-based security policy and send portions thereof to enforcement points along a path configured for an entity to access a resource. For example, a portion of a security policy corresponding to an operation may be mapped to and implemented by an enforcement point having a capability to perform the operation. Once each operation of a security policy has been mapped to an enforcement point, a chain of enforcement points may be generated.

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