UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,
- vs. -
CENTRIPETAL NETWORKS, INC.,
Patent Owner

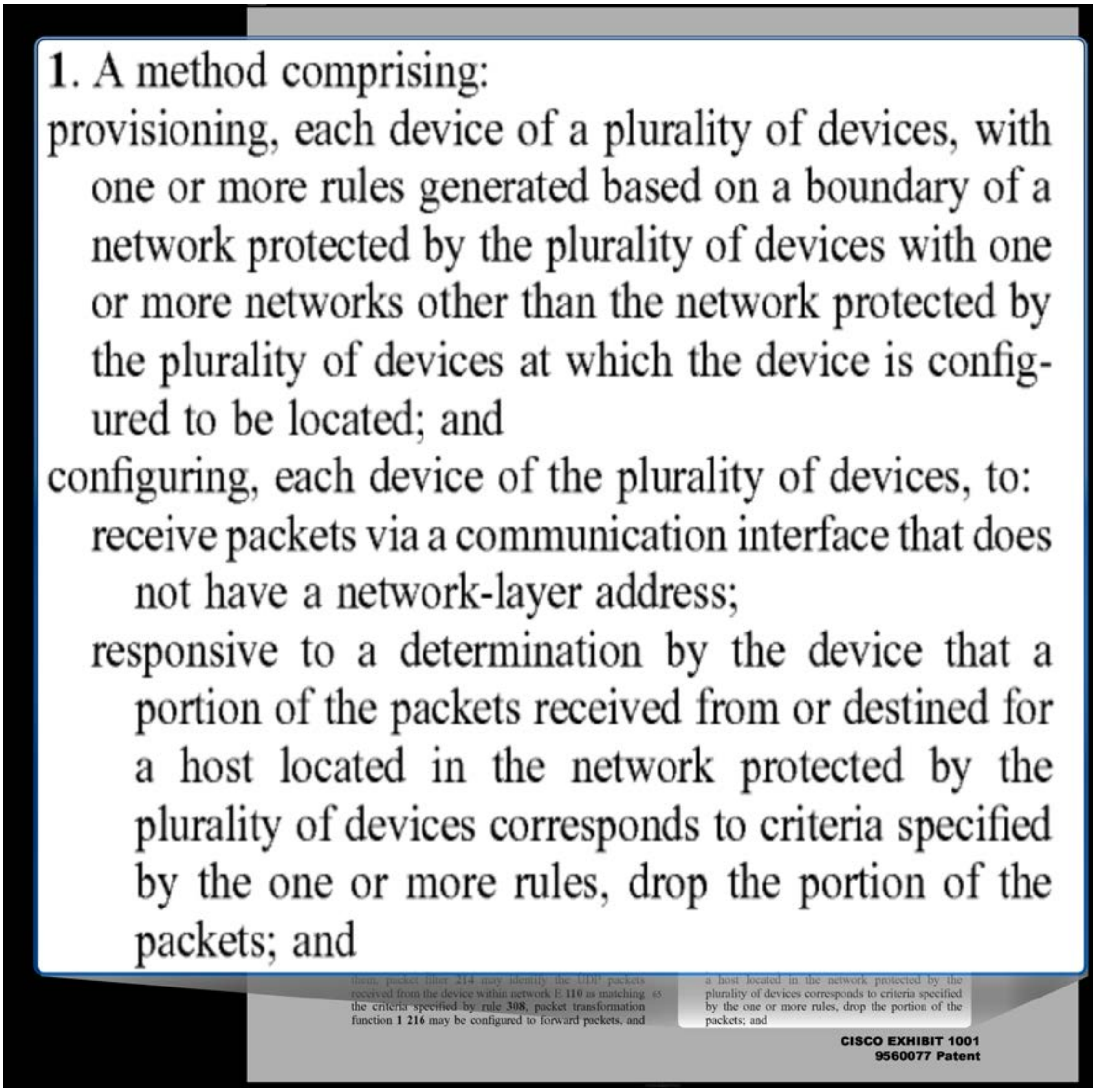
Case No.: IPR2018-01513

US Patent 9,560,077

# PETITIONER'S DEMONSTRATIVE EXHIBITS

PTAB ORAL ARGUMENT

January 9, 2020



1. A method comprising:

provisioning, each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located; and

configuring, each device of the plurality of devices, to:

receive packets via a communication interface that does not have a network-layer address;

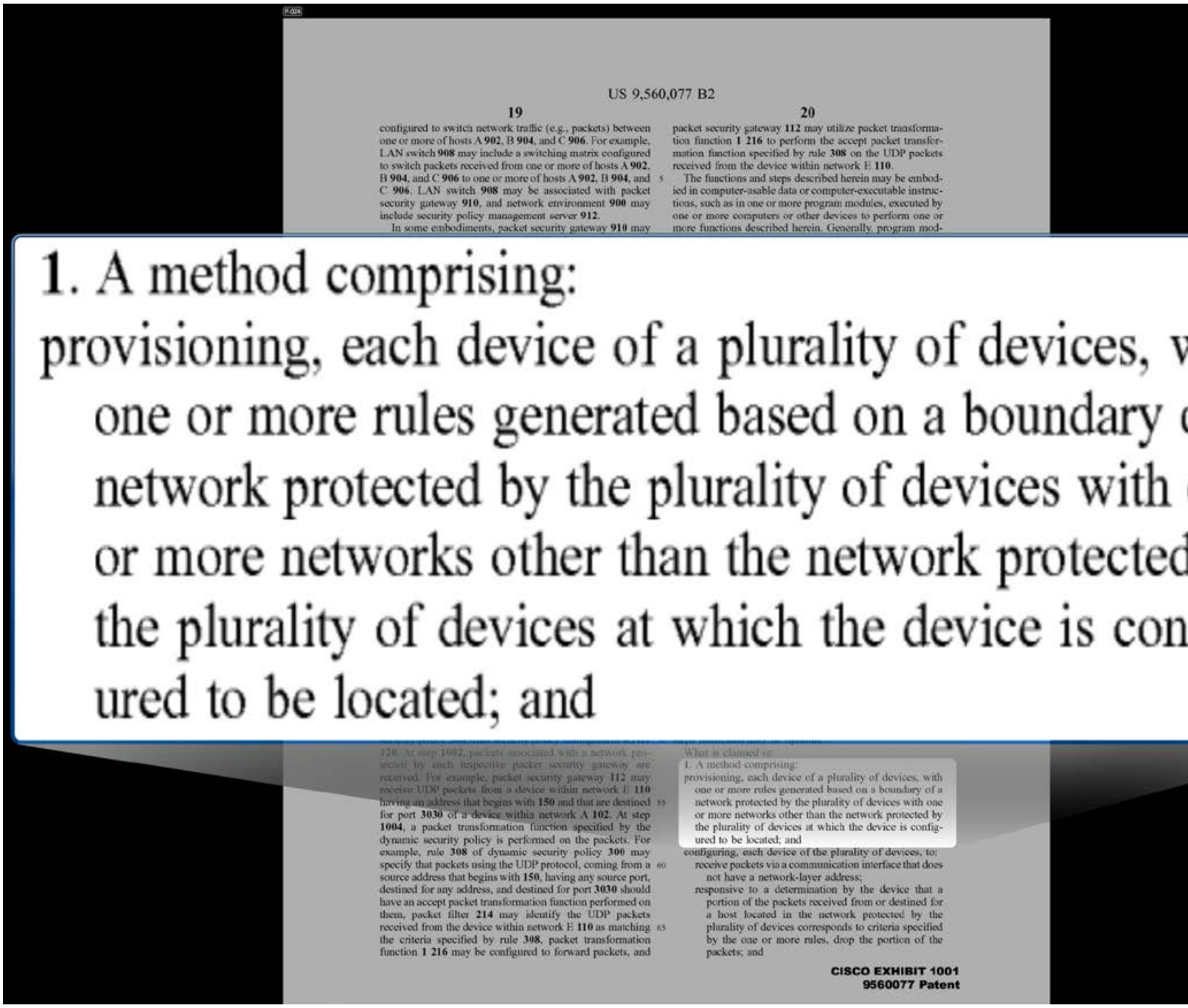
responsive to a determination by the device that a portion of the packets received from or destined for a host located in the network protected by the plurality of devices corresponds to criteria specified by the one or more rules, drop the portion of the packets; and

them, packet filter **214** may identify the UDP packets received from the device within network E **110** as matching the criteria specified by rule **308**, packet transformation function **1 216** may be configured to forward packets, and

a host located in the network protected by the plurality of devices corresponds to criteria specified by the one or more rules, drop the portion of the packets; and

**CISCO EXHIBIT 1001**
**9560077 Patent**

EX1001, Col. 20:52-67



P-024

US 9,560,077 B2

19

configured to switch network traffic (e.g., packets) between one or more of hosts A **902**, B **904**, and C **906**. For example, LAN switch **908** may include a switching matrix configured to switch packets received from one or more of hosts A **902**, B **904**, and C **906** to one or more of hosts A **902**, B **904**, and C **906**. LAN switch **908** may be associated with packet security gateway **910**, and network environment **900** may include security policy management server **912**.

In some embodiments, packet security gateway **910** may

120. At step 1002, packets associated with a network protected by each respective packet security gateway are received. For example, packet security gateway **112** may receive UDP packets from a device within network E **110** having an address that begins with **150** and that are destined for port **3030** of a device within network A **102**. At step **1004**, a packet transformation function specified by the dynamic security policy is performed on the packets. For example, rule **308** of dynamic security policy **300** may specify that packets using the UDP protocol, coming from a source address that begins with **150**, having any source port, destined for any address, and destined for port **3030** should have an accept packet transformation function performed on them, packet filter **214** may identify the UDP packets received from the device within network E **110** as matching the criteria specified by rule **308**, packet transformation function **1 216** may be configured to forward packets, and

20

packet security gateway **112** may utilize packet transformation function **1 216** to perform the accept packet transformation function specified by rule **308** on the UDP packets received from the device within network E **110**.

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 mod-

What is claimed is:

1. A method comprising:

provisioning, each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located; and

configuring, each device of the plurality of devices, to:

receive packets via a communication interface that does not have a network-layer address;

responsive to a determination by the device that a portion of the packets received from or destined for a host located in the network protected by the plurality of devices corresponds to criteria specified by the one or more rules, drop the portion of the packets; and

CISCO EXHIBIT 1001
9560077 Patent

1. A method comprising:

provisioning, each device of a plurality of devices, w

one or more rules generated based on a boundary o

network protected by the plurality of devices with o

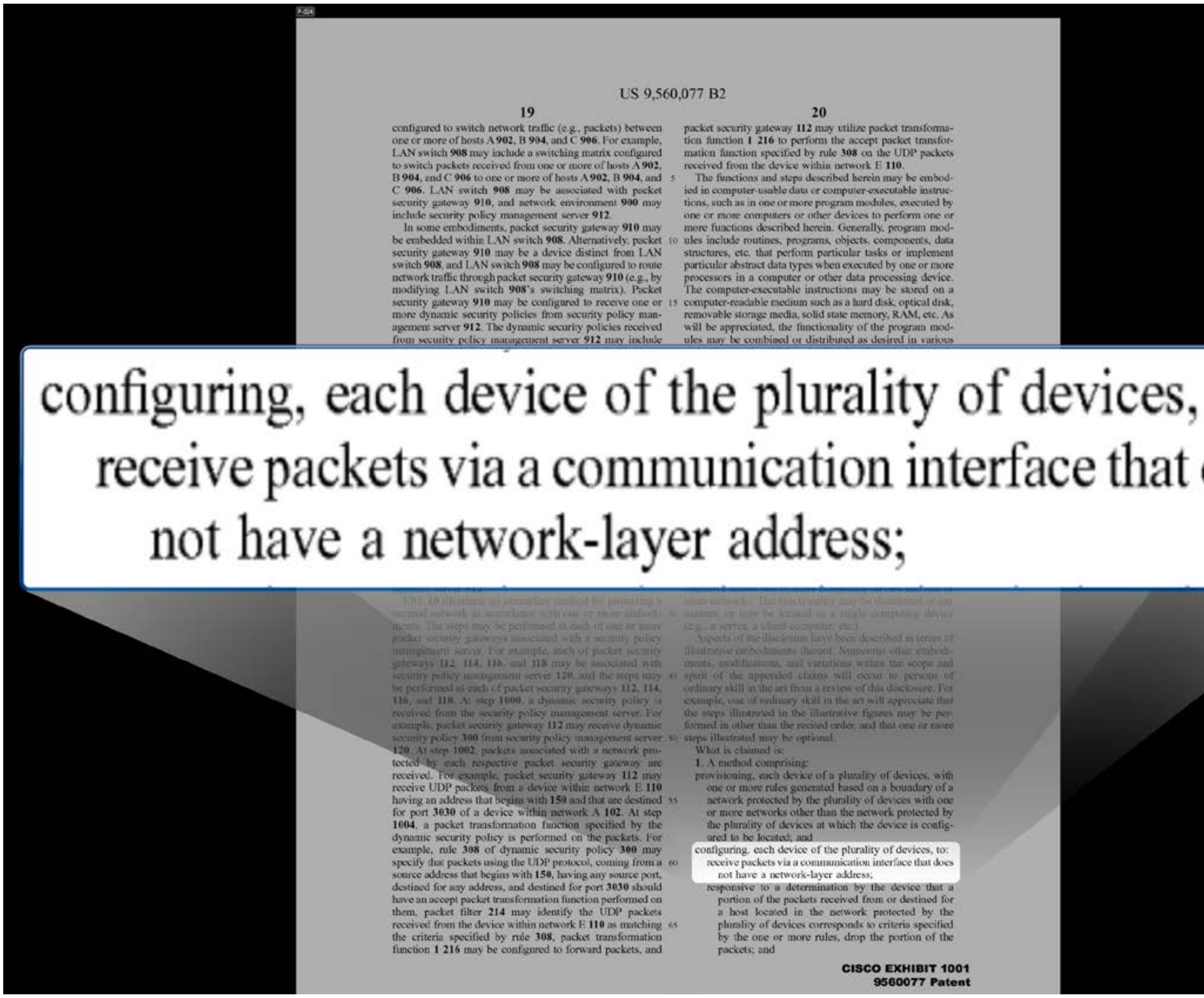
or more networks other than the network protected

the plurality of devices at which the device is con

ured to be located; and

EX1001, Col

**DEMONSTRATIVE EXHIBIT – NOT EVIDENCE**



US 9,560,077 B2

19

configured to switch network traffic (e.g., packets) between one or more of hosts A 902, B 904, and C 906. For example, LAN switch 908 may include a switching matrix configured to switch packets received from one or more of hosts A 902, B 904, and C 906 to one or more of hosts A 902, B 904, and C 906. LAN switch 908 may be associated with packet security gateway 910, and network environment 900 may include security policy management server 912.

In some embodiments, packet security gateway 910 may be embedded within LAN switch 908. Alternatively, packet security gateway 910 may be a device distinct from LAN switch 908, and LAN switch 908 may be configured to route network traffic through packet security gateway 910 (e.g., by modifying LAN switch 908's switching matrix). Packet security gateway 910 may be configured to receive one or more dynamic security policies from security policy management server 912. The dynamic security policies received from security policy management server 912 may include

FIG. 10 illustrates an exemplary method for protecting a secured network in accordance with one or more embodiments. The steps may be performed at each of one or more packet security gateways associated with a security policy management server. For example, each of packet security gateways 112, 114, 116, and 118 may be associated with security policy management server 120, and the steps may be performed at each of packet security gateways 112, 114, 116, and 118. At step 1000, a dynamic security policy is received from the security policy management server. For example, packet security gateway 112 may receive dynamic security policy 300 from security policy management server 120. At step 1002, packets associated with a network protected by each respective packet security gateway are received. For example, packet security gateway 112 may receive UDP packets from a device within network E 110 having an address that begins with 150 and that are destined for port 3030 of a device within network A 102. At step 1004, a packet transformation function specified by the dynamic security policy is performed on the packets. For example, rule 308 of dynamic security policy 300 may specify that packets using the UDP protocol, coming from a source address that begins with 150, having any source port, destined for any address, and destined for port 3030 should have an accept packet transformation function performed on them, packet filter 214 may identify the UDP packets received from the device within network E 110 as matching the criteria specified by rule 308, packet transformation function 1 216 may be configured to forward packets, and

20

packet security gateway 112 may utilize packet transformation function 1 216 to perform the accept packet transformation function specified by rule 308 on the UDP packets received from the device within network E 110.

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 various

more networks. The functionality may be distributed in any manner, or may be located in a single computing device (e.g., a server, a client computer, etc.).

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 steps illustrated may be optional.

What is claimed is:

1. A method comprising:

provisioning, each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located; and

configuring, each device of the plurality of devices, to:

receive packets via a communication interface that does not have a network-layer address;

responsive to a determination by the device that a portion of the packets received from or destined for a host located in the network protected by the plurality of devices corresponds to criteria specified by the one or more rules, drop the portion of the packets; and

CISCO EXHIBIT 1001
9560077 Patent

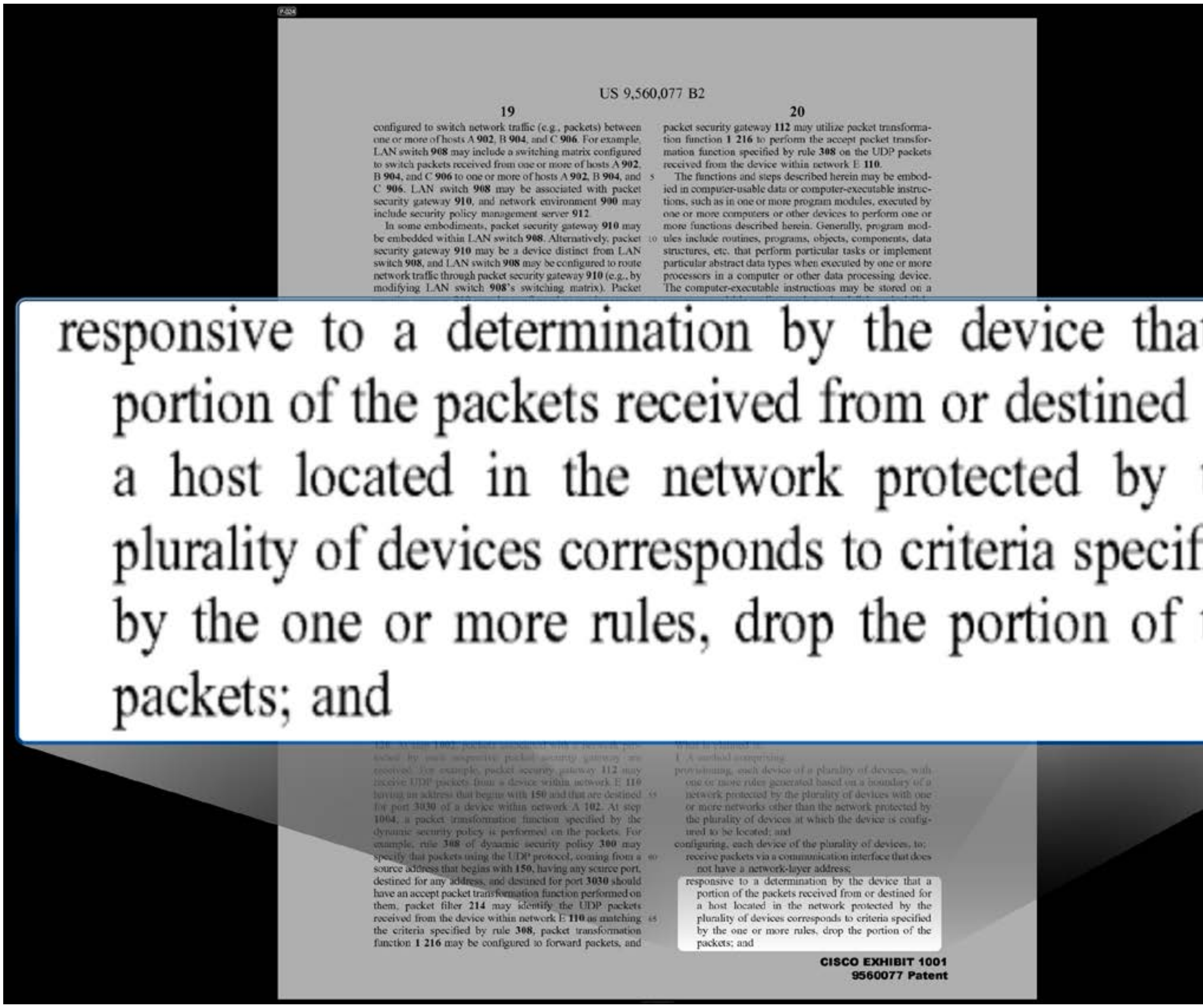
configuring, each device of the plurality of devices,

receive packets via a communication interface that

not have a network-layer address;

EX1001, Col.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE



responsive to a determination by the device tha
portion of the packets received from or destined
a host located in the network protected by
plurality of devices corresponds to criteria specif
by the one or more rules, drop the portion of
packets; and

US 9,560,077 B2

19

configured to switch network traffic (e.g., packets) between one or more of hosts A 902, B 904, and C 906. For example, LAN switch 908 may include a switching matrix configured to switch packets received from one or more of hosts A 902, B 904, and C 906 to one or more of hosts A 902, B 904, and C 906. LAN switch 908 may be associated with packet security gateway 910, and network environment 900 may include security policy management server 912.

In some embodiments, packet security gateway 910 may be embedded within LAN switch 908. Alternatively, packet security gateway 910 may be a device distinct from LAN switch 908, and LAN switch 908 may be configured to route network traffic through packet security gateway 910 (e.g., by modifying LAN switch 908's switching matrix). Packet

120. At step 1002, packets associated with a network protected by each respective packet security gateway are received. For example, packet security gateway 112 may receive UDP packets from a device within network E 110 having an address that begins with 150 and that are destined for port 3030 of a device within network A 102. At step 1004, a packet transformation function specified by the dynamic security policy is performed on the packets. For example, rule 308 of dynamic security policy 300 may specify that packets using the UDP protocol, coming from a source address that begins with 150, having any source port, destined for any address, and destined for port 3030 should have an accept packet transformation function performed on them, packet filter 214 may identify the UDP packets received from the device within network E 110 as matching the criteria specified by rule 308, packet transformation function 1 216 may be configured to forward packets, and

20

packet security gateway 112 may utilize packet transformation function 1 216 to perform the accept packet transformation function specified by rule 308 on the UDP packets received from the device within network E 110.

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

What is claimed is:

1. A method comprising:

provisioning, each device of a plurality of devices, with one or more rules generated based on a boundary of a network protected by the plurality of devices with one or more networks other than the network protected by the plurality of devices at which the device is configured to be located; and

configuring, each device of the plurality of devices, to:

receive packets via a communication interface that does not have a network-layer address;

responsive to a determination by the device that a portion of the packets received from or destined for a host located in the network protected by the plurality of devices corresponds to criteria specified by the one or more rules, drop the portion of the packets; and

CISCO EXHIBIT 1001
9560077 Patent

EX1001, Col.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

### LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

### FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

### E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

**WHAT WILL YOU BUILD?** | **sales@docketalarm.com** | **1-866-77-FASTCASE**