Trials@uspto.gov
571-272-7822

Paper 7
Entered: April 2, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case IPR2018-01513
Patent 9,560,077 B2

Before BRIAN J. McNAMARA, J. JOHN LEE, and
JOHN P. PINKERTON, *Administrative Patent Judges*.

LEE, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
35 U.S.C. § 314

INTRODUCTION

Cisco Systems, Inc. ("Petitioner") filed a Petition (Paper 2, "Pet.") requesting an *inter partes* review of claims 1–20 ("the challenged claims") of U.S. Patent No. 9,560,077 B2 (Ex. 1001, "the '077 Patent"). Centripetal Networks, Inc. ("Patent Owner") timely filed a Preliminary Response (Paper 6, "Prelim. Resp.").

We have authority to institute an *inter partes* review only if the information presented in the Petition shows "there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a). An *inter partes* review may not be instituted on fewer than all claims challenged in the Petition. *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018).

Upon consideration of the Petition and Preliminary Response, we determine that the information presented shows there is a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of each of the challenged claims. Accordingly, we institute an *inter partes* review of the challenged claims of the '077 Patent.

A. Related Cases

The parties identify as related to the present case *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case No. 2:18-cv-00094-MSD-LRL (E.D. Va). Pet. 1; Paper 3, 1.

B. The '077 Patent

The '077 Patent relates to protecting networks using packet security gateways (PSGs) armed with dynamic security policies. Ex. 1001, 1:48–61. Figure 1 of the '077 Patent is reproduced below:

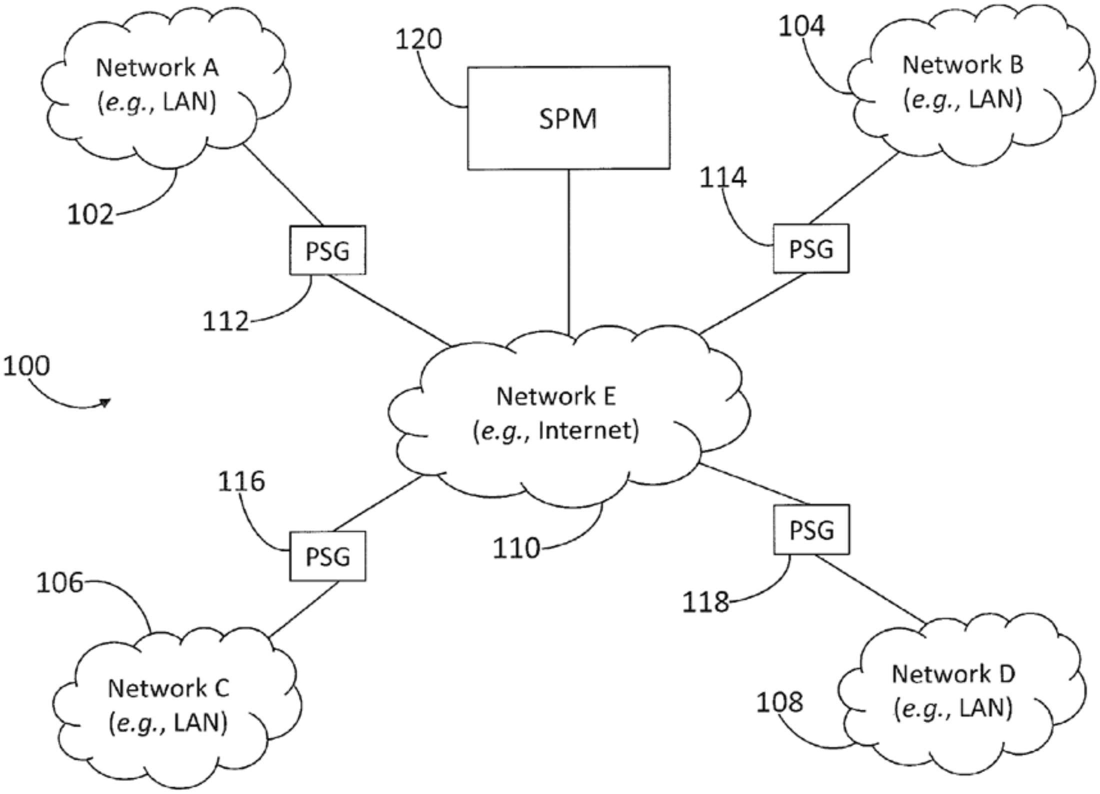

FIG. 1

Figure 1 illustrates network environment 100 in which aspects of the claimed invention of the ’077 Patent are implemented, with networks 102, 104, 106, 108, and 110 interfacing with each other. *Id.* at 4:27–30, 4:38–40. For example, one or more Internet Service Providers (ISPs) in network environment 100 may interface one or more networks via the Internet. *Id.* at 4:40–45. PSG 112 is located at the boundary between Network A 102 and Network E 110. *Id.* at 5:11–15. Network A 102 may be, for example, a Local Area Network (LAN) associated with an organization or other entity. *Id.* at 4:30–37. Each PSG receives a dynamic security policy from security policy management (SPM) server 120. *Id.* at 5:29–31.

PSG 112 may include a packet filter that examines information associated with data packets received by the PSG via its network interfaces with network A and network E. *Id.* at 5:66–6:10, Fig. 2. The packet filter may be configured with a dynamic security policy that includes one or more rules, each of which may specify criteria and an action to be taken on data packets meeting the criteria. *Id.* at 6:11–31. Such actions may include forwarding or dropping the packets. *Id.* at 6:19–27. In addition, PSG 112 may be configured in a "network layer transparent manner," i.e., without a network layer address, to be insulated against attacks launched at the network layer. *Id.* at 6:32–46.

C. Challenged Claims

Petitioner challenges all of the claims of the '077 Patent. Claims 1, 7, 13, 19, and 20 are the independent claims. Claim 1 is illustrative and is reproduced below:

> 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
> >
> > modify a switching matrix of a local area network (LAN) switch associated with the device such that the LAN

> switch is configured to drop the portion of the packets responsive to the determination by the device.

D. Asserted Ground of Unpatentability and Asserted Prior Art

Petitioner asserts that claims 1–4, 6–10, 12–16, 18, and 20 are unpatentable as obvious under 35 U.S.C. § 103(a) in view of Jungck.[1] Pet. 20. Further, Petitioner contends claims 5, 11, 17, and 19 are unpatentable as obvious under 35 U.S.C. § 103(a) in view of the combination of Jungck and RFC 2003.[2] *Id*. In addition, Petitioner relies on the Declaration of Kevin Jeffay, Ph.D. (Ex. 1004), in support of both asserted grounds of unpatentability.

ANALYSIS

A. Claim Construction

For petitions filed before November 13, 2018, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016). The parties propose constructions for several claim terms.

[1] U.S. Patent Application Pub. No. 2009/0262741 A1, published Oct. 22, 2009 (Ex. 1008, "Jungck").

[2] C. Perkins, *IP Encapsulation within IP*, Oct. 1996 (Ex. 1009, "RFC 2003"). At this stage of the case, Patent Owner has not disputed Petitioner's assertion that RFC 2003 qualifies as prior art. For purposes of this Decision, we determine Petitioner has made a sufficient showing that RFC 2003 is prior art to the '077 Patent.

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