Trials@uspto.gov
571-272-7822

Paper 14
Entered: November 15, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ZSCALER INC.,
Petitioner,

v.

SYMANTEC CORPORATION,
Patent Owner.

Case IPR2018-00930
Patent 8,402,540 B2

Before JEFFREY S. SMITH, BRYAN F. MOORE, and NEIL T. POWELL, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*.

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

I. INTRODUCTION

Zscaler Inc. ("Petitioner") requests *inter partes* review of claims 1–18 of U.S. Patent No. 8,402,540 B2 ("the '540 patent," Ex. 1001) pursuant to

35 U.S.C. §§ 311 *et seq*. Paper 1 ("Pet."). Petitioner relies on the testimony of Dr. Markus Jakobsson. Ex. 1003. Symantec Corporation ("Patent Owner") filed a preliminary response. Paper 10 ("Prelim. Resp."). Institution of an *inter partes* review is authorized by statute when "the information presented in the petition . . . and any response . . . shows that 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); *see* 37 C.F.R. § 42.108. Upon consideration of the Petition and Preliminary Response, we conclude the information presented shows there is not a reasonable likelihood that Petitioner would prevail in establishing the unpatentability of claims 1–18 of the '540 patent.

A. Related Matters

A decision in this proceeding could affect or be affected by the following cases pending in the United States District Court for the Northern District of California and involving the '540 patent: *Symantec Corp. and Symantec Ltd. v. Zscaler, Inc.*, Case No. 17-cv-04414 (N.D. Cal.); *Symantec Corp. and Symantec Ltd. v. Zscaler, Inc.*, Case No. 17-cv-04426 (N.D. Cal.). Pet. 2; Paper 3, 2.

B. The '540 patent

The '540 patent relates generally to protecting computer systems from viruses, attacks from hackers, spyware, spam, and other malicious activities. Ex. 1001, 1:65–2:4. A flow processing facility inspects payloads of network traffic packets and provides security and protection to a computer. Abstract. Figure 1 of the '540 patent is reproduced below.

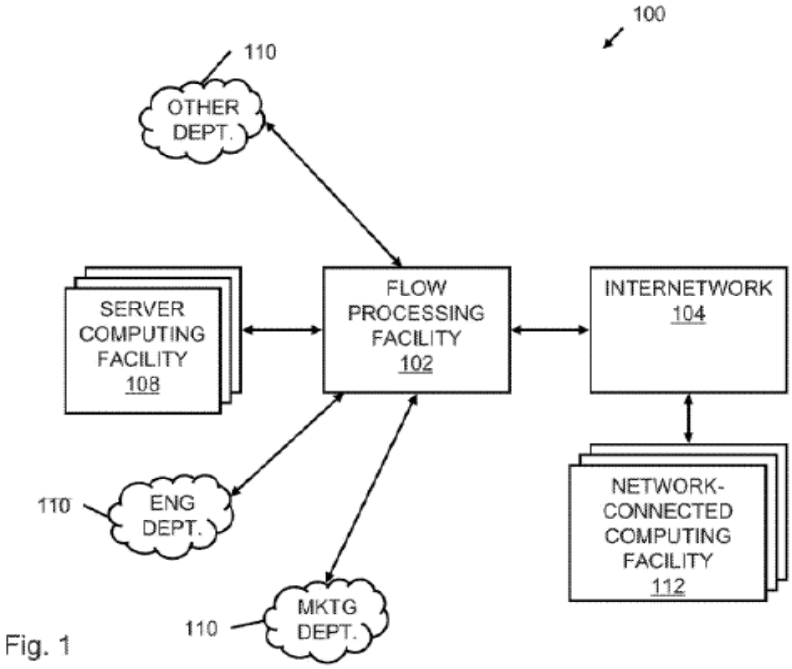

Fig. 1

Figure 1 above shows a networked computing environment 100 for data flow processing, including flow processing facility 102 coupled to internetwork 104, a network-connected computing facility 112, a plurality of server computing facilities 108, and a number of departmental computing facilities 110, such as an engineering department, a marketing department, and another department. Ex. 1001, 19:28–41. Flow processing facility 102 receives data flows from the computing facilities via internetwork 104 and processes the data flows. *Id*. at 20:16–20.

Figure 30 below shows a schematic of an enterprise network. *Id*. at 85:50–55.

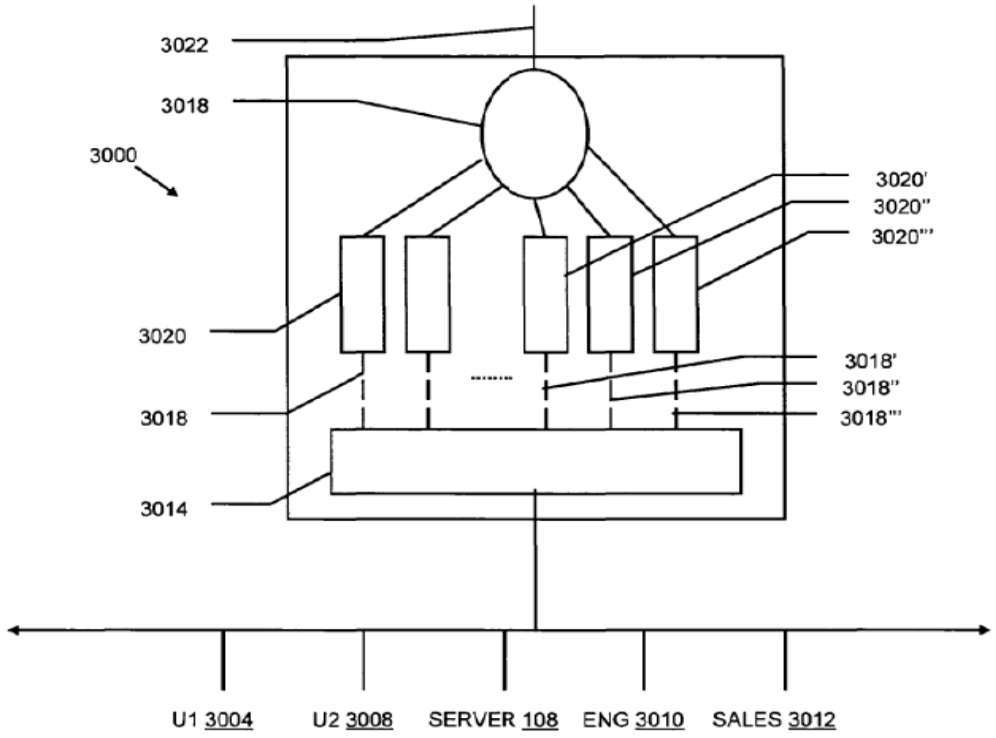

FIG. 30

Figure 30 above shows network participants of network 3000 include user1 3004, user2 3008, and server 108, and participant types of network 3000 include engineering 3010 and sales 3012. *Id.* at 85:65–86:8. Virtualization model 3014 of flow processing facility 102 uniquely identifies data flows 444 from each participant and routes the data flow to a virtual network 3018 associated with the virtual network. *Id.* at 86:26–30. Security policy 3020 is applied to data flow 444 of virtual network 3018, such as anti-virus, anti-span, anti-spyware, and anti-worm. *Id.* at 86:43–49.

C. Illustrative Claim

Independent claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A method of securing a plurality of virtual networks with a virtualized network security system (VNSS), comprising:

providing a plurality of flow processors, each configured as elements of the VNSS for processing a data flow, said data flow being transferred between a first port and a second port of the VNSS, the data flow comprising subscriber profile data;

establishing a first security policy for a first virtual network based at least in part on the subscriber profile data

included in the data flow;

establishing a second security policy for a second virtual network based at least in part on the subscriber profile data included in the data flow;

processing the data flow received at said first port for the first and second virtual networks through at least one of the plurality of flow processors, wherein portions of the data flow that are associated with the first virtual network are processed according to the first security policy, and wherein portions of the data flow that are associated with the second virtual network are processed according to the second security policy, said processing further comprising:

making a first determination, in accordance with one of the first security policy and the second security policy, of abnormalities that are associated with the data flow, the first determination based at least in part on the subscriber identified by the subscriber profile data; and

making a second determination, in accordance with one of the first security policy and the second security policy, based at least in part on the subscriber identified by the subscriber profile data, and transferring said data flow to said second port.

Ex. 1001, 119:16–49.

DOCKET ALARM

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.