Trials@uspto.gov
571-272-7822

Paper 50
Filed: October 16, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ZSCALER, INC.,
Petitioner,

v.

SYMANTEC CORPORATION,
Patent Owner.

IPR2018-00913
Patent 8,316,429 B2

Before NEIL T. POWELL, DANIEL N. FISHMAN, and MINN CHUNG, *Administrative Patent Judges*.

FISHMAN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. *Background and Summary*

Zscaler, Inc. ("Petitioner") filed a Petition (Paper 1, "Petition" or "Pet.") requesting *inter partes* review of claims 10–12 (the "challenged claims") of U.S. Patent No. 8,316,429 B2 ("the '429 patent," Ex. 1001) pursuant to 35 U.S.C. §§ 311 *et seq*. Symantec Corporation ("Patent Owner") filed a Preliminary Response. Paper 10 ("Prelim. Resp.").

On October 17, 2018, based on the record before us at that time, we instituted an *inter partes* review of all challenged claims on all grounds of unpatentability asserted in the Petition. Paper 13 ("Decision on Institution" or "Dec. on Inst.").

Patent Owner filed a Response (Paper 17, "PO Resp."), Petitioner filed a Reply (Paper 26, "Reply"), and Patent Owner filed a Sur-Reply (Paper 35, "Sur-Reply").[1]

The parties filed several unopposed motions to seal various papers and exhibits to protect alleged confidential information. *See* Papers 16, 25, 34, 42, 44, 47. We address these motions below.

Upon consideration of the complete record, we determine by a preponderance of the evidence that claims 10–12 are unpatentable.

B. *Real Parties in Interest*

Petitioner identifies Zscaler, Inc. as the sole real party in interest for Petitioner. Pet. 2. Patent Owner identifies Symantec Corporation and

[1] Patent Owner also filed a redacted version of its Response (Paper 18) and a redacted version of its Sur-Reply (Paper 36), and Petitioner filed a redacted version of its Reply (Paper 27), the redacted versions filed to protect alleged confidential information.

Symantec Limited as the real parties in interest for Patent Owner. Paper 6, 2.

C. Related Matters

The parties inform us that the '429 patent is presently asserted against Petitioner in the following litigation: *Symantec Corp. v. Zscaler, Inc.*, Case No. 3:17-cv-04414-JST (N.D. Cal.) (transferred from 1:17-cv-00806-MAK in the District of Delaware). Pet. 2; Paper 6, 2. Petitioner further identifies two other *inter partes* reviews directed to claims of other patents of Patent Owner as well as a second petition challenging claims 1–9 and 13–17 of the '429 patent. Pet. 3 (citing Cases IPR2018-00616, IPR2018-00806, and IPR2018-00912). Petitioner also identifies another litigation involving other patents of Patent Owner (*Symantec Corp. v. Zscaler, Inc.*, 17-cv-04426 (N.D. Cal.) (transferred from 16-cv-01176 in the District of Delaware)). Patent Owner further identifies litigation 1:17-cv-00432-VAC-SRF involving the '429 patent and IPR2018-00912 requesting review of certain claims of the '429 patent. Paper 6, 2.

D. The '429 Patent

The '429 patent discloses that firewalls are common in computing networks to implement policies that determine which network traffic can pass between two network systems by blocking certain exchanges when one or more policies applicable to the information to be exchanged are not met. Ex. 1001, 1:14–22. Such firewalls are often implemented in a proxy server intermediate between two networks attempting to exchange information. *Id.* at 1:23–24. The firewall/proxy server intercepts information to be exchanged and examines the information to evaluate it against firewall rules/policies to determine whether the exchange should be allowed. *Id.* at 1:30–34.

According to the '429 patent, some applications, such as banking or e-commerce over the Internet, encrypt the information exchanges to protect sensitive information. *Id.* at 1:34–40. The '429 patent explains that such encrypted communications usually cannot be read by the firewall and, thus, cannot be evaluated against rules/policies of the firewall to determine whether to allow or block the exchange. *Id.* at 1:41–50. According to the '429 patent, one possible solution is to permit the proxy to decrypt the encrypted communications and then evaluate the decrypted communication against the firewall policies. *Id.* at 1:51–55. The '429 patent notes that such a solution is undesirable because, once decrypted, the communications could be attacked to improperly obtain private information (such as banking information of a customer). *Id.* at 1:55–2:3.

The '429 patent purports to address these security needs by intercepting secure (encrypted) communications and evaluating the intercepted information with respect to policies of the firewall without decrypting the communications. *Id.* at 2:30:39. Specifically, in an embodiment of the '429 patent, a Uniform Resource Locator ("URL") of a host computer involved in a communication is extracted from a digital certificate associated with the host, and the host is categorized based on the extracted URL. *Id.* at 2:30–33. The '429 patent discloses an embodiment in which systems communicate using the Secure Socket Layer ("SSL") standard protocol. *See id.* at 1:6–10. Figure 1 of the '429 patent is reproduced below.

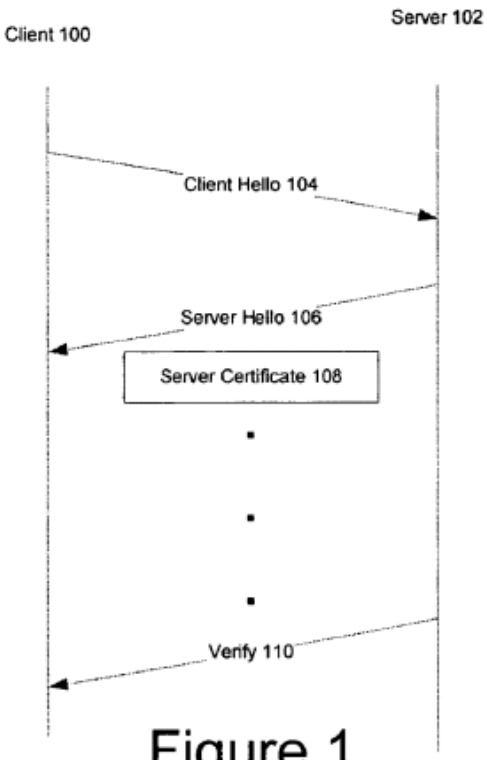

Figure 1

Figure 1 shows a conventional SSL handshake protocol between a client and a server, as known in the art. *Id.* at 3:11–12. Client 100 initiates a secure connection by sending client hello message 104 to server 102, which responds with server hello message 106. *Id.* at 4:40–43. Server hello message 106 includes server certificate 108. *Id.* at 4:45–48. In an embodiment, "[t]he present invention makes use of information in the Certificate Info field of the server's digital certificate to identify the host the client is contacting and, based on that identification, determine whether or not SSL communications may be passed encrypted through a firewall at a proxy." *Id.* at 5:34–38.

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.