Trials@uspto.gov
571-272-7822

Paper 8
Entered: August 24, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SOPHOS LTD. and SOPHOS INC.,
Petitioner,

v.

FORTINET, INC.,
Patent Owner.

Case IPR2015-00911
Patent 8,205,251 B2

Before MICHAEL R. ZECHER, MATTHEW R. CLEMENTS, and MINN CHUNG, *Administrative Patent Judges*.

CLEMENTS, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Sophos Ltd. and Sophos Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1, 6, 9, 12, 17, 18, 22, 26, 27, 29, 31 and 32 (“the challenged claims”) of U.S. Patent No. 8,205,251 B2 (Ex. 1001, “the ’251 patent”). Paper 1 (“Pet.”). Fortinet, Inc. (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may be authorized only if “the information presented in the petition . . . and any [preliminary] 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). Upon consideration of the Petition and the Preliminary Response, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing in showing the unpatentability of any of the challenged claims of the ’251 patent. Accordingly, we do not institute an *inter partes* review for any of the challenged claims.

A. Related Proceedings

The ’251 patent is involved a co-pending district court case in the U.S. District Court for District of Delaware. Pet. 1; Paper 5, 2. Petitioner also filed petitions in Cases IPR2015-00910 and IPR2015-00912 involving related U.S. Patent Nos. 7,966,654 B2 and 8,656,479 B2, respectively. Paper 5, 2.

B. The ’251 Patent

The ’251 patent relates generally to network security and specifically to application-level content processing of network service protocols using a firewall. Ex. 1001, 1:23–26. According to the ’251 patent, “critical network threats, like viruses and worms, are embedded in the application-level contents of packet streams.” *Id.* at 1:36–38. Moreover, “[m]any existing firewall systems use global configuration settings, such as global lists of [Uniform Resource Locators] to block, lists of spam addresses, options to scan for viruses, spam, and other similar parameters,” and “[t]hese settings are applied globally to all policies within the firewall.” *Id.* at 2:6–10. Such an approach, according to the ’251 patent, did not provide administrators with sufficient flexibility to, for example, block certain members, but not others, from accessing certain websites. *Id.* at 2:11–23.

The ’251 patent describes a firewall system in which a configuration scheme is associated with a specific firewall policy and, when a new communication session matching the firewall policy is initiated, the proxy program to which the communication connection is redirected looks up the scheme settings from a configuration database. *Id.* at 4:52–66. Figure 1 of the ’251 patent is reproduced below:

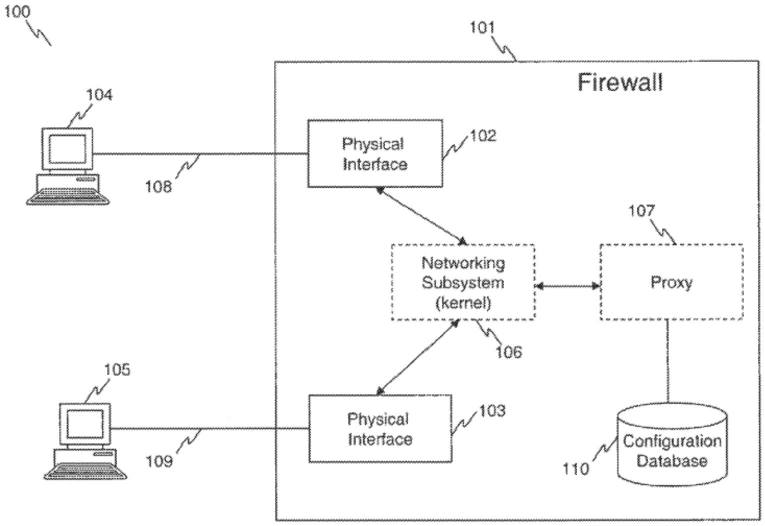

Figure 1

Figure 1 illustrates a topology of firewall-protected network 100 in accordance with an embodiment of the ’251 patent. *Id.* at 5:3–5. Firewall 101 is disposed within the network communication channel between two user systems 104 and 105, and monitors network packet exchanges between them. *Id.* at 5:16–19. Network subsystem 106 may redirect packets to proxy 107, which then builds and interprets the data buffer. *Id.* at 5:37–40. Specifically, proxy 107 assembles the formatted packets intercepted by networking subsystem 106 in accordance with the specification of the respective communication protocol to arrive at the transmission content. *Id.* at 6:5–9. Configuration database 110 stores various firewall policies, configuration schemes, and other parameters used by firewall system 101. *Id.* at 6:13–15. The stored parameters are retrieved from configuration database 110 by proxy 107. *Id.* at 6:15–16.

Figure 2 of the ’251 patent is reproduced below.

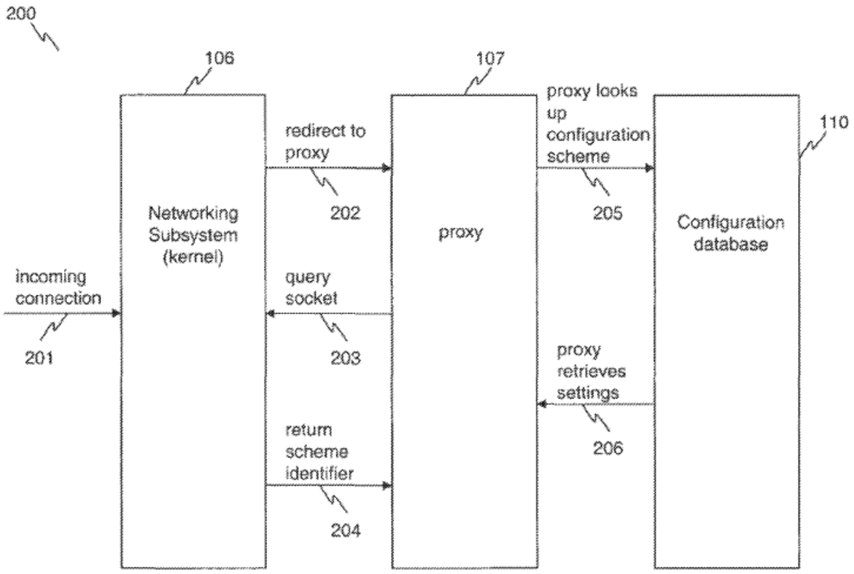

Figure 2

Figure 2 illustrates an operating sequence of firewall system 101 when establishing a basic network communication session. *Id.* at 6:30–32.

Incoming connection 201 is accepted by networking subsystem 106 after a lookup of an applicable firewall policy. *Id.* at 6:32–34. The policy indicates that the session should be redirected to proxy 107, as shown in step 202. *Id.* at 6:34–36. Proxy 107 queries the kernel (step 203) to retrieve the configuration scheme associated with the session. *Id.* at 6:36–39. Once retrieved (step 204), proxy 107 queries (step 205) configuration database 110 to retrieve the settings for the configuration scheme matching the specified identifier. *Id.* at 6:39–42. Once the settings are retrieved (step 206), proxy 107 continues with filtering tasks or other tasks necessary to handle the network session. *Id.* at 6:42–45.

C. Illustrative Claim

Of the challenged claims, claims 1, 17, and 26 are independent. Claim 1 is reproduced below:

> 1. A computer-implemented method for processing application-level content of network service protocols, the method comprising:
>
> redirecting a network connection, by a networking subsystem implemented within a kernel of an operating system of a firewall device, to a proxy module of one or more proxy modules within the firewall device that is configured to support a network service protocol associated with the network connection;
>
> retrieving, by the proxy module, one or more content processing configuration schemes associated with a matching firewall policy for the network service protocol and the network connection, the one or more content processing configuration schemes each including a plurality of content processing configuration settings for each of one or more network service protocols; and

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**