

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner

v.

BT AMERICAS INC.,
Patent Owner

Case No. IPR2023-00889
U.S. Patent No. 7,895,641

**PETITIONER'S REPLY
TO PATENT OWNER'S PRELIMINARY RESPONSE**

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	The claimed “analysis of post-filtering residue” does not exclude additional filtering.....	1
II.	PO attempts to import unclaimed requirements into the “identify[ing] potentially security-related events” element.....	2
III.	PO’s interpretation of “dynamically modifying” is overly narrow.	4

The Board should institute this proceeding. As discussed further below, Patent Owner (“PO”) seeks to improperly narrow the claims in an attempt to overcome the prior art, but even under PO’s flawed interpretation that conflicts with its own positions in prior litigation, the prior art relied upon in this proceeding still teaches the claim elements.

I. The claimed “analysis of post-filtering residue” does not exclude additional filtering.

PO suggests that the claimed “analysis of post-filtering residue” must occur after *all* possible filtering operations, and “[a]ny mid-filtering data still being considered is not yet ‘post-filtering’ data.” POPR, 40-41. Such a construction is inconsistent with both the plain meaning and the previous district-court claim construction ruling, which PO agrees should apply. POPR, 40-41.

In previous district-court litigation against third party Fortinet, the court construed “post-filtering residue” as “status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering.” EX1013, 4. Nowhere does the court’s construction require, as PO argues here, that the “residue” cannot be subject to further filtering as part of the analysis, as long as that analysis occurs *after* (i.e., “post”) the negative and positive filtering. And here, PO does not challenge that Duvall’s initial ALLOW and BLOCK filters are forms of “negative and positive filtering” under the district court’s previous construction. *See* POPR, 37-42.

This understanding is also consistent with the plain meaning of “post-filtering.” The ’641 patent describes, for example, performing stages of “negative filtering” and “positive filtering,” followed by further analysis by an “anomaly engine.” EX1001, 8:51-62. The ’641 patent does not explain or restrict what type of analysis may be performed by the “anomaly engine”—only that it “determines what residue information may be worthy of additional analysis,” which may include additional filtering. *Id.* The patent does not use the term “mid-filtering,” much less distinguish between “post-filtering” and “mid-filtering” analysis.

Regardless, the Duvall reference discloses exactly what PO alleges the claims require—“the filtering process to produce the residue, [and] that it be ‘followed by’ a separate analysis performed on the post-filtering residue.” POPR, 33. There is no dispute that Duvall’s deferred action analysis, as depicted in Duvall’s Figure 4, is a separate analysis performed *after* Duvall determines whether immediate action (ALLOW and BLOCK filtering) is required. Pet., 15-18; EX1003, ¶¶103-105.

II. PO attempts to import unclaimed requirements into the “identify[ing] potentially security-related events” element.

In yet another attempt to avoid institution, PO raises multiple claim construction-related issues, improperly adding new, unclaimed requirements.

First, PO asserts, “[n]either [Duvall nor Chu] analyzes any data to identify *potential* threats after filtering (*i.e.*, previously unknown threats from the post-

filtering residue).” POPR, 38 (emphasis in original). But the claims do not require “potentially security-related events” to be “previously unknown threats,” as PO contends. *Id.* The term “unknown” appears nowhere in the ’641 patent claims. The term appears only three times in the specification and never as a defining characteristic of “potentially security-related events.” EX1001, 21:37, 23:31, 26:45. Rather, the ’641 patent describes “potential security-related event[s]” in a broader fashion, merely referring to activity that is inconclusive of a security-related event. *See, e.g.*, EX1001, 5:44-49 (“data *possibly indicating* an unauthorized intrusion or other security-related event...”) (emphasis added).

Regardless, the prior art teaches “identify[ing] potentially security-related events” under PO’s narrow construction. The purpose of Duvall’s deferred filtering analysis is to identify threats that do not match Duvall’s initial “ALLOW or BLOCK filters”—i.e., unknown threats. Pet., 16-18; EX1003, ¶¶103-105. Known threats would have been blocked at this initial step while permitted data would have been allowed. Duvall’s deferred action step analyzes any residual data using, for example, “keyword” and “pattern” matching (including using “a wildcard character”) to identify any potential threats that were not originally blocked by the BLOCK filters—i.e., unknown threats. EX1004, 5:8-19, 6:19-41 (identifying transmissions to/from sources that include “a potentially objectionable phrase” such as “sex” or “xxx”); Pet., 17-18; EX1003, ¶¶104-105.

Second, the claims do not require that “potentially security-related events” be determined by “[o]bjective analysis,” as PO now contends. POPR, 39-40. The patent, in fact, says that its data analysis is merely based on determining whether information is “interesting,” “uninteresting,” or “worthy of additional analysis,” with no further specificity. EX1001, 8:51-62. Nevertheless, Duvall’s filtering is not based on “subjective preferences.” POPR, 39. For example, Duvall discloses providing “a uniform set of filters for many users” in a corporate environment, and filtering “outlaw[ed]” material. Pet., 23-24, 26, 36 (citing EX1004, 1:18-24, 8:21-23).

Third, PO argues that identification of “objectionable/non-objectionable material” is not “security-related.” POPR, 39-40. But the ’641 patent does not limit the scope of what may be considered “security-related.” In fact, the ’641 patent states that “the present invention is usable generally for [] monitoring of any system.” EX1001, 15:59-67; Pet., 8. Still, Dr. Jeffay explains that Duvall’s and Chu’s techniques apply to other security-related contexts, and that objectionable material also presents virus- and malware-related risks. EX1003, ¶¶117-118, 138.

III. PO’s interpretation of “dynamically modifying” is overly narrow.

Under the district court’s previous claim construction ruling (on which PO’s arguments are allegedly premised), “dynamically” merely means “during actual operation, rather than offline.” POPR, 48; EX1013, 2. PO, however, attempts to

read this term more narrowly to exclude basic database operations well known in the art, implying the term refers to some new technical improvement. Not so.

Neither the specification nor prosecution history support that “dynamic” modification refers to a novel technical operation. The ’641 patent states that its filters “may be manually updated offline or dynamically (that is, during actual operation)” but provides *no further detail* about how the updates may be performed “during actual operation,” EX1001, 5:32-35—rightfully suggesting that “dynamic” updating was common and well known. Pet., 41-42; EX1003, ¶¶149-153.

As Petitioner’s expert, Dr. Jeffay, explains, updating during actual operation is a “known database editing technique[.]” EX1003, ¶¶151-153 (citing EX1004, 8:10-11). In other words, a POSITA would have recognized that standard operation would allow a database to be written without taking it offline. EX1003, ¶¶151-153. PO does not argue the contrary. Instead, PO argues that such operation is not inherent. POPR, 49-50. But whether such operation is inherent is irrelevant and not required by the claims. The Petition and Dr. Jeffay provide reasons why it would be advantageous—and, therefore, obvious—to update Duvall’s database without taking it offline, which is indisputably a well-known database operation. Pet., 41-42; EX1003, ¶¶149-53.

For the forgoing reasons and the reasons set forth in the Petition, the Board should institute this proceeding and find all challenged claims unpatentable.

Respectfully submitted,
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

/Jonathan Tuminaro/

Jonathan Tuminaro (Reg. No. 61,327)
Michael D. Specht (Reg. No. 54,463)
Daniel Block (Reg. No. 68,395)
Steven M. Pappas (Reg. No. 73,904)
Attorneys for Petitioner Palo Alto Networks, Inc.

Date: September 22, 2023

1101 K Street, N.W., 10th Floor
Washington, D.C. 20005-3934
(202) 371-2600

CERTIFICATION OF SERVICE

The undersigned hereby certifies that the foregoing **PETITIONER’S
REPLY TO PATENT OWNER’S PRELIMINARY RESPONSE** was served electronically via e-mail on September 22, 2023 in its entirety on the following counsel for Patent Owner:

Nolan M. Goldberg (Lead Counsel) NGoldbergPTABMatters@proskauer.com
Baldassare Vinti (Back-up Counsel) BVinti@proskauer.com
Jonathan A. Roberts (Back-up Counsel) jr@nixonvan.com
Raymond Y. Mah (Back-Up Counsel) rym@nixonvan.com
Joseph A. Rhoa (Back-up Counsel) jar@nixonvan.com
PROSKAUER ROSE LLP
NIXON & VANDERHYE P.C.

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

/Jonathan Tuminaro/

Jonathan Tuminaro
Registration No. 61,327
Attorney for Petitioner Palo Alto Networks, Inc.

Date: September 22, 2023

1101 K Street, N.W., 10th Floor
Washington, D.C. 20005-3934
(202) 371-2600