

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

Case No. IPR2021-01154
Patent No. 10,785,266

**PATENT OWNER'S PRELIMINARY RESPONSE
UNDER 37 C.F.R. § 42.107**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. THE BOARD SHOULD DENY THE PETITION UNDER 35 U.S.C. § 314(a).....	3
A. The Board Should Deny Institution in View of the Advanced Stage of the Co-Pending Litigation.....	3
1. Factor 1: The Unlikely Potential for a Stay Weighs in Favor of Denying Institution.....	3
2. Factor 2: The Early Trial Date Weighs in Favor of Denying Institution	4
3. Factor 3: The Significant Investment in Parallel Proceedings Weighs in Favor of Denying Institution.....	4
4. Factors 4 & 5: Overlapping Issues and Parties Weigh in Favor of Denying Institution.....	6
5. Petitioner's Dilatory Conduct Weighs in Favor of Denying Institution	7
B. The Board Should Deny Institution in View of Petitioner's Recurrent Word Count Violations	8
III. THE '266 PATENT.....	11
A. Overview	11
B. Prosecution History	14
IV. CLAIM CONSTRUCTION	16
V. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 325(d).....	17
A. The Same or Substantially the Same Art and Arguments Were Previously Presented to the Office	18

1.	The Office Already Determined that <i>Jungck</i> Does Not Disclose the “Entire Boundary” and “All Traffic” Limitations	18
2.	<i>Jungck</i> ’s “Virus Watch Service” is Substantially Similar to and Cumulative of Bhatnagar	21
3.	The Patent Office Previously Considered Substantially the Same Art as <i>Wood</i> and <i>Sarathy</i>	22
B.	Petitioner Does Not Show that the Patent Office Materially Erred	25
1.	Petitioner Does Not Acknowledge the Office’s Prior Consideration of <i>Jungck</i> With Respect to the “Entire Interface” and “All Traffic” Limitations	26
2.	Petitioner Does Not Demonstrate Material Error in the Examiner’s Consideration of <i>Jungck</i> Regarding the Malicious Host Tracker Elements.....	28
VI.	THE CHALLENGED CLAIMS ARE PATENTABLE	31
A.	<i>Jungck</i> Does Not Disclose the “Entire Interface” or “All Traffic” Limitations.....	32
1.	<i>Jungck</i> Fails to Disclose the “Entire Interface” Limitation	34
2.	<i>Jungck</i> Does Not Disclose the All Traffic Limitation	39
	(a) <i>Jungck</i> ’s client requests do not traverse a boundary of a network protected by the packet security gateway.....	39
	(b) <i>Jungck</i> ’s edge caches bypass the edge servers and some traffic avoids the edge server’s rules.	41
	(c) <i>Jungck</i> ’s edge server does not apply “one or more packet filtering rules” on to “all traffic traversing the boundary.”	45

3.	Petitioner’s Obviousness Grounds Do Not Adequately Explain Its Combinations, Including for the “All Traffic” and “Entire Interface” Limitations.....	48
(a)	Petitioner’s generic motivations to combine <i>Jungck</i> ’s embodiments are conclusory and insufficiently specific to the claims.	48
(b)	Petitioner’s motivations in the claim chart also have no meaningful connection to the claims, including the “entire interface” and “all traffic” limitations.....	52
B.	Petitioner Has Not Demonstrated that the Art Discloses an SPMS Automatically Creating or Altering Rules	58
C.	Petitioner Has Not Shown that <i>Jungck</i> ’s External Devices Update Rules Based on “Updated Malicious Traffic Information” Received from a “Malicious Host Tracker Service”	60
VII.	CONCLUSION.....	63

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Abiomed, Inc. v. Maquet Cardiovascular, LLC</i> , IPR2017-01204, Paper 8 (P.T.A.B. Oct. 23, 2017).....	53
<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH</i> , IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020).....	<i>passim</i>
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020).....	3, 5, 8
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015)	51
<i>Belden Techs. Inc. v. Superior Essex Commc'ns LP</i> , No. 08-63-SLR, 2010 WL 3522327 (D. Del. Sept. 2, 2010).....	8
<i>Bio-Rad Labs., Inc. v. 10X Genomics</i> , IPR2019-00567, Paper 23 (P.T.A.B. Aug. 8, 2019).....	6
<i>Boston Scientific Scimed, Inc. v. Cordis Corp.</i> , 554 F.3d 982 (Fed. Cir. 2009) (Pet.).....	56
<i>Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.</i> , 289 F.3d 801 (Fed. Cir. 2002)	16, 17
<i>Centripetal Networks, Inc. v. Palo Alto Networks, Inc.</i> , No. 2:21-cv-00137-RCY-RJK (E.D. Va. Mar. 12, 2021)	1
<i>Cisco Sys., Inc. v. C-Cation Techs., LLC</i> , IPR2014-00454, Paper 12 (P.T.A.B. Aug. 29, 2014).....	10
<i>Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.</i> , IPR2020-00122, Paper 15 (P.T.A.B. May 15, 2020)	4
<i>Comair Rotron, Inc. v. Nippon Densan Corp.</i> , IPR2020-00122, Paper 15 (P.T.A.B. May 15, 2020)	32
<i>Costco Wholesale Corp. v. Robert Bosch LLC</i> , IPR2016-00042, Paper 28 (P.T.A.B. July 7, 2016).....	52, 58

<i>EHS Lens Philippines, Inc. v. Essilor Int'l</i> , No. 3:16-cv-00563-JAG, 2016 WL 11670108 (E.D. Va. Sept. 22, 2016).....	4
<i>EMC Corp. v. Intell. Ventures I LLC</i> , IPR2017-00429, Paper 11 (P.T.A.B. July 5, 2017).....	9
<i>Google Inc. v. Ji-Soo Lee</i> , IPR2016-00022, Paper 25 (P.T.A.B. Nov. 23, 2016).....	10
<i>Hulu, LLC v. Sound View Innovations, LLC</i> , IPR2018-00582, Paper 34 (P.T.A.B. Aug. 5, 2019).....	49
<i>Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.</i> , 381 F.3d 1111 (Fed. Cir. 2004)	59
<i>Innovations4Flooring NV v. Välinge Innovation AB</i> , IPR2017-02130, Paper 8 (P.T.A.B. Feb. 7, 2018).....	10
<i>Intell. Bio-Sys., Inc. v. Illumina Cambridge, Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	48, 51
<i>Johns Manville Corp. v. Knauf Insulation, Inc.</i> , IPR2018-00827, Paper 9 (P.T.A.B. Oct. 16, 2018).....	48, 58
<i>Kinetic Concepts, Inc. v. Smith & Nephew, Inc.</i> , 688 F.3d 1342 (Fed. Cir. 2012)	57
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	48, 53
<i>Limelight Networks, Inc. v. Akamai Techs., Inc.</i> , IPR2016-01894, Paper 8 (P.T.A.B. Mar. 8, 2017)	10
<i>In re Meng</i> , 492 F.2d 843 (C.C.P.A. 1974)	35
<i>Mercedes-Benz USA, LLC v. Stragent, LLC</i> , IPR2021-00426, Paper 13 (P.T.A.B. July 19, 2021).....	27
<i>Metalcraft of Mayville, Inc. v. Toro Co.</i> , 848 F.3d 1358 (Fed. Cir. 2017)	48

<i>Mylan Pharm., Inc. v. Bayer Intell. Prop. GmbH</i> , IPR2018-01143, Paper 13 (P.T.A.B. Dec. 3, 2018)	7
<i>NHK Spring Co. v. Intri-Plex Tech.</i> , IPR2018 00752, Paper 8 (P.T.A.B. Sept. 12, 2018).....	7
<i>Panduit Corp. v. Corning Optical Commc'ns LLC</i> , IPR2017-00528, Paper 7 (P.T.A.B. May 30, 2017)	10
<i>PayPal, Inc. v. IOENGINE, LLC</i> , IPR2019-00930, Paper 16 (P.T.A.B. Oct. 29, 2019).....	52
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	51
<i>Pollard Banknote Ltd. v. Nanografix Corp.</i> , IPR2019-01288, Paper 10 (P.T.A.B. Jan. 8, 2020)	51
<i>Regeneron Pharms., Inc. v. Novartis Pharma AG</i> , IPR2020-01317, Paper 15 (P.T.A.B. Jan. 15, 2021)	5
<i>Samsung SDI Co. v. UBE Indus., Inc.</i> , IPR2017-02116, Paper 8 (P.T.A.B. Mar. 12, 2018).....	53
<i>Sand Revolution II, LLC v. Cont'l Intermodal Grp. — Trucking LLC</i> , IPR2019-01393, Paper 24 (P.T.A.B. June 16, 2020)	5
<i>Segin Sys., Inc. v. Stewart Title Guaranty Co.</i> , 30 F. Supp. 3d 476 (E.D. Va. 2014)	5
<i>SIBIA Neurosciences, Inc. v. Cadus Pharm. Corp.</i> , 225 F.3d 1349 (Fed. Cir. 2000)	57
<i>In re Stepan Co.</i> , 868 F.3d 1342 (Fed. Cir. 2017)	53
<i>In re Suong-Hyu Hyon</i> , 679 F.3d 1363 (Fed. Cir. 2012)	57
<i>Universal Imaging Indus., LLC v. Lexmark Int'l, Inc.</i> , IPR2019-01383, Paper 7 (P.T.A.B. Feb. 27, 2020).....	22, 51

<i>Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	17
--	----

<i>In re Wesslau</i> , 353 F.2d 238 (C.C.P.A. 1965)	37
--	----

Statutes

35 U.S.C. § 314(a)	1, 3, 6, 7, 8
35 U.S.C. § 325(d)	2, 17, 18, 26, 27

Other Authorities

37 C.F.R. § 42.5	10
37 C.F.R. § 42.6(a)(3)	10
37 C.F.R. § 42.12(b)(8)	10
Federal Rules of Civil Procedure 26(f)	7
Federal Rules of Civil Procedure 30(b)(6)	4
Manual of Patent Examining Procedure § 609.02 (9th ed. Rev. 10.2019, June 2020)	20
Manual of Patent Examining Procedure § 2001.06(b) (9th ed. Rev. 10.2019, June 2020)	20
Manual of Patent Examining Procedure § 2144.04 (9th ed. Rev. 10.2019, June 2020)	59

PATENT OWNER'S EXHIBIT LIST

Exhibit	Description
2001	Declaration of Hannah Lee in Support of Plaintiff Centripetal Networks, Inc.'s Opposition to Defendant Palo Alto Networks, Inc.'s Motion to Stay with Exhibits 1 and 4, <i>Centripetal Networks, Inc. v. Palo Alto Networks, Inc.</i> , Case No. 2:21-cv-00137 (RCY), Dkt. No. 86 (E.D. Va. July 23, 2021)
2002	Protective Order, <i>Centripetal Networks, Inc. v. Palo Alto Networks, Inc.</i> , Case No. 2:21-cv-00137-RCY-RJK, Dkt. No. 93 (E.D. Va. July 30, 2021) ("Protective Order")
2003	Amended Complaint for Patent Infringement, <i>Centripetal Networks, Inc. v. Palo Alto Networks, Inc.</i> , Case No. 2:21-cv-00137-RCY, Dkt. No. 65 (E.D. Va. July 9, 2021) ("Amended Complaint")
2004	Order Regarding Discovery of Electronically Stored Information ("ESI"), <i>Centripetal Networks, Inc. v. Palo Alto Networks, Inc.</i> , Case No. 2:21-cv-00137-AWA-RJK, Dkt. No. 155 (E.D. Va. Sept. 13, 2021) ("ESI Order")
2005	Memorandum in Support of Defendant's Motion to Stay Pending Resolution of <i>Inter Partes</i> Review Proceedings, <i>Centripetal Networks, Inc. v. Palo Alto Networks, Inc.</i> , Case No. 2:21-cv-00137-RCY-RJK, Dkt. No. 68 (E.D. Va. July 9, 2021)
2006	Declaration of James Hannah in Support of Patent Owner's Preliminary Response
2007	U.S. Patent No. 10,567,437 (the "'437 Patent")
2008	File History for U.S. Patent No. 10,567,437

Exhibit	Description
2009	U.S. Patent Application Publication No. 2003/0118038 A1 (“Jalava”)
2010	Transcript of deposition of Dr. Kevin Jeffay from <i>Cisco Sys., Inc. v. Centripetal Networks, Inc.</i> , No. IPR2018-01513, taken on June 28, 2019
2011	Transcript of deposition of Dr. Kevin Jeffay from <i>Cisco Sys., Inc. v. Centripetal Networks, Inc.</i> , No. IPR2018-01513, taken on November 27, 2019
2012	U.S. Patent Application Publication No. 2006/123481 A1 (“Bhatnagar”)
2013	U.S. Patent No. 10,091,246 (the “’246 Patent”).
2014	Patent Owner’s Response Under 37 C.F.R. § 42.107, <i>Cisco Systems, Inc. v. Centripetal Networks, Inc.</i> , No. IPR2018-01443, Paper 12 (P.T.A.B. May 13, 2019)
2015	U.S. Patent. Application Publication No. 2010/0082811 A1 (“Van Der Merwe”)
2016	Petition for <i>Inter Partes</i> Review, <i>Palo Alto Networks, Inc. v. Centripetal Networks, Inc.</i> , No. IPR2021-01153, Paper 2 (P.T.A.B. July 6, 2021)
2017	Order, <i>Bushnell Hawthorne, LLC v. Cisco Sys., Inc.</i> , Case No. 1:18 cv-00760, Dkt. No. 88 (E.D. Va. Apr. 22, 2019)
2018	Memorandum Order, <i>Cont’l Auto. Sys., Inc. v. Hamaton Auto. Tech. Co.</i> , Case No. 2:16-cv-00226, Dkt. No. 63 (E.D. Va. Feb. 7, 2017)

I. INTRODUCTION

Palo Alto Networks, Inc., (“Petitioner”) petitioned for *inter partes* review of claims 1–27 of U.S. Patent No. 10,785,266 (Ex. 1001, the “’266 Patent”). The Board should deny institution.

Petitioner rushed to prepare the petition to bolster its case for a stay in the co-pending litigation: *Centripetal Networks, Inc. v. Palo Alto Networks, Inc.*, No. 21-cv-00137-RCY-RJK (E.D. Va. Mar. 12, 2021). Because that stay is unlikely to be granted under the circumstances, the Board should exercise its discretion under 35 U.S.C. § 314(a) and deny institution. Institution would waste the Board’s resources given the parallel litigation in the Eastern District of Virginia’s “rocket docket,” which is scheduled to go to trial six months before the Final Written Decision (“FWD”) is due in this case.

Petitioner’s haste is evident from its slapdash claim charts, relying almost entirely on conclusory collateral estoppel arguments stemming from prior IPR proceedings involving U.S. Patent Nos. 9,137,205 (the “’205 Patent”) and 9,560,077 (the “’077 Patent”). Collateral estoppel cannot not apply, however, because the Challenged Claims include the following limitations absent from the ’205 and ’077 Patents:

- (1) “a plurality of packet security gateways that ***collectively provide an entire interface across a boundary*** of a network protected by the packet security gateway” (the “entire interface” limitation);

- (2) “a first set of packet filtering rules to be applied to ***all network traffic traversing the boundary***” (the “all traffic” limitation);
- (3) “one or more first packet filtering rules... automatically created or altered by the security policy management server based on aggregated malicious traffic information received from at least one third party malicious host tracker service” (the “automatic rule” limitation); or
- (4) “one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service” (the “automatic updating” limitation).

Nor has Petitioner has shown these limitations are taught by *Jungck* (Ex. 1051, U.S. Patent Application Publication No. 2009/0262741), *Wood* (Ex. 1052, U.S. Patent Application Publication No. 2007/0097976), and/or *Sarathy* (Ex. 1063, U.S. Patent Application Publication No. 2009/0249482).

To the contrary, the Board should exercise its discretion to deny the Petition under 35 U.S.C. § 325(d) because the Examiner already considered *Jungck* extensively with respect to the “entire boundary” and “all traffic” elements during consideration of the '266 Patent's parent, U.S. Patent No. 10,567,437 (“the '437 Patent”). Petitioner fails to apprise the Board of this critical aspect of the Office's prior consideration of *Jungck* with respect to these two limitations let alone demonstrate any error in the Examiner's treatment. Further, the *Jungck*, *Wood*,

and *Sarathy* are cumulative to the art that the Examiner applied to the “automatic rule” and “automatic updating” limitations during prosecution of the '266 Patent.

II. THE BOARD SHOULD DENY THE PETITION UNDER 35 U.S.C. § 314(a)

A. The Board Should Deny Institution in View of the Advanced Stage of the Co-Pending Litigation

The *Fintiv* factors weigh in favor of the Board's exercise of discretionary denial based on the advanced stage of the parallel district court proceeding. See *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 5–6 (P.T.A.B. Mar. 20, 2020) (precedential).

1. Factor 1: The Unlikely Potential for a Stay Weighs in Favor of Denying Institution

As is typical of defendants in co-pending district court litigation, Petitioner filed a motion to stay the district court litigation based on its IPRs on July 9, 2021. That motion is pending, and the district court has neither ruled on the motion to stay nor indicated when it may rule or that a stay will even be granted even if this proceeding is instituted. Indeed, in the Eastern District of Virginia, stays requested before institution are routinely denied. See, e.g., *EHS Lens Philippines, Inc. v. Essilor Int'l*, No. 3:16-cv-00563-JAG, 2016 WL 11670108, at *1 (E.D. Va. Sept. 22, 2016); Ex. 2017 at 1.

2. Factor 2: The Early Trial Date Weighs in Favor of Denying Institution

Should trial be instituted, the earliest FWD in this IPR proceeding would not be issued until January 2023, six months after the anticipated trial date of August 1, 2022. Petition (Paper 2, “Pet.”) at 7; Ex. 2001 (Declaration of Hannah Lee) at 1, ¶ 2; *id.* at 19–20. Factor 2 thus favors denying institution. *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15 at 7–8 (P.T.A.B. May 15, 2020) (denying institution with a trial date set approximately 6 months prior to the FWD deadline).

3. Factor 3: The Significant Investment in Parallel Proceedings Weighs in Favor of Denying Institution

Factor 3 similarly favors denying institution because the parties have already invested substantial time and resources in the litigation. Discovery is underway as both parties have served several sets of discovery requests and responses amounting to 238 requests for production, 20 requests for admission, and 28 interrogatories over the last several months ago beginning on July 6, 2021, as well as initial disclosures on July 16, 2021 that identified relevant witnesses and categories of documents. Ex. 2001 at 2, ¶¶ 3–4; Ex. 2006 (Declaration of James Hannah), ¶ 2. And, on October 19, 2021, Patent Owner served a Fed. R. Civ. P. 30(b)(6) notice of deposition on Petitioner. Ex. 2006, ¶ 3. The parties negotiated and filed a stipulated Protective Order and ESI Order, both entered by the Court on

July 30, 2021 and September 13, 2021, respectively. Ex. 2002; Ex. 2004. The parties agreed to a *Markman* hearing at the end of March 2022, and substantial fact discovery will be completed by the time the Board would have determined whether to institute on this petition. Ex. 2001 at 19.

The Board routinely denies institution given this type of significant investment. *See Regeneron Pharms., Inc. v. Novartis Pharma AG*, IPR2020-01317, Paper 15 at 15–17 (P.T.A.B. Jan. 15, 2021) (denying institution and finding *Fintiv* Factor 3 was in favor of denying institution because the parties had already responded to 365 requests for production, 43 interrogatories, and produced thousands of documents and by the time of institution there would be substantially more exchange of expert and fact discovery causing the ITC considerable resources to date); *see also Sand Revolution II, LLC v. Cont'l Intermodal Grp.—Trucking LLC*, IPR2019-01393, Paper 24 at 10–11 (P.T.A.B. June 16, 2020) (The Board found *Fintiv* 3 factor weighed in favor of denying institution because the parties expended significant investment in discovery despite the district court not yet having expended much effort on invalidity.).

Moreover, the Eastern District of Virginia routinely denies stays in cases at stages similar to this one, further strengthening both this Factor and Factor 1. *Segin Sys., Inc. v. Stewart Title Guaranty Co.*, 30 F. Supp. 3d 476, 481–82 (E.D. Va. 2014) (denying motion to stay where trial date had been set, discovery had

recently begun, *Markman* hearing had been set, and scheduled trial would occur months before PTAB would finish its review); Ex. 2018 at 6.

4. Factors 4 & 5: Overlapping Issues and Parties Weigh in Favor of Denying Institution

The parties are identical between the district court litigation and this IPR proceeding, and Petitioner asserts the same prior art in the Petition in the litigation. While Petitioner has stated in its pending motion to stay that after a FWD, it will be estopped from asserting in litigation any ground that it raised or reasonably could have raised during the IPR proceedings, it has not filed a stipulation with the Board.

As Petitioner is well aware, by the time a FWD issues, the trial will likely have already occurred in the district court litigation, making Petitioner's stipulation moot. There is no reasonable need for the parties and the Board to expend significant resources in this IPR proceeding and the co-pending district court litigation, where the same invalidity defenses, will need to be litigated. The *Markman* hearing is anticipated to occur in March 2022, and the district court will have issued a claim construction order well before the PTAB issues a FWD. When there is such overlap with a co-pending validity challenge before another court, the Board has exercised its discretion under § 314(a) to deny institution. See *Bio-Rad Labs., Inc. v. 10X Genomics*, IPR2019-00567, Paper 23, 27–29 (P.T.A.B. Aug. 8, 2019) (denying institution under § 314(a) where a parallel ITC proceeding

considered a validity challenge using the same references as in the IPR petition); *Mylan Pharm., Inc. v. Bayer Intell. Prop. GmbH*, IPR2018-01143, Paper 13 at 12–14 (P.T.A.B. Dec. 3, 2018) (denying institution under § 314(a) where petitioner relies on the same references in district court that it relies on in the petition); *NHK Spring Co. v. Intri-Plex Tech.*, IPR2018 00752, Paper 8 at 18–20 (P.T.A.B. Sept. 12, 2018) (same). Thus, these factors favor discretionary denial.

5. Petitioner's Dilatory Conduct Weighs in Favor of Denying Institution

Petitioner's dilatory conduct is another factor that weighs in favor of denying institution. Petitioner has repeatedly tried to delay the co-pending litigation to better position itself to argue against a discretionary denial.

Patent Owner served Petitioner with its complaint and amended complaint in March and June 2021, respectively. Rather than answer, Petitioner moved to dismiss and then refused to conduct a Fed. R. Civ. P. 26(f) conference citing its motion as the reason. *See* Ex. 2001 at 9. Following this tactic, Petitioner filed seven IPR petitions over the course of two weeks, stating that it would file more IPRs as to seven additional asserted patents. However, these filings until four months after the litigation began despite having prior knowledge of Patent Owner and its patents before the litigation. Ex. 2003, ¶¶ 64–77.

In Exhibit C to the Joint Rule 26(f) Report and Proposed Discovery Plan sent in July 2021, Petitioner proposed later dates for claim construction and

discovery in an attempt to avoid discretionary denial of its IPR petitions and to use those IPRs to stay the litigation. Ex. 2001 at 19, 23–25. But for these dilatory tactics, the litigation would have been even further along than its already advanced stage. Ex. 2005 at 6–9. Petitioner's intentional retardation of the district court proceedings must not be considered a factor in its favor; indeed the Board should infer that Petitioner has been "seeking an inappropriate tactical advantage."

Belden Techs. Inc. v. Superior Essex Commc'ns LP, No. 08-63-SLR, 2010 WL 3522327, at *2 (D. Del. Sept. 2, 2010) (stay denied).

In addition, Petitioner's counsel is subject to a pending motion to disqualify the co-pending district court litigation, calling into question the viability of this Petition in light of the significant conflict of interest. Thus, this factor favors denying institution.

* * *

All six *Fintiv* factors warrant denying institution. The Board should use its discretionary authority under § 314(a) to deny the petition.

B. The Board Should Deny Institution in View of Petitioner's Recurrent Word Count Violations

Petitioner certifies that its petition "contains 13,977 words yet Patent Owner's word processing software counted 14,215 words, excluding exempted portions. Pet. at Certificate of Compliance. And if that were not enough, the petition would have included at least an additional three-hundred words had

Petitioner not improperly truncated citations. *See generally* Pet. (using improperly truncated exhibit numbers such as “EX1001,” citing exhibit authors or titles rather than a proper exhibit number, and omitting spaces after citations with “¶” and “FIG” throughout); *EMC Corp. v. Intell. Ventures I LLC*, IPR2017-00429, Paper 11 at 27–29 (P.T.A.B. July 5, 2017) (“Petitioner’s use of atypical citations amounts to formatting tricks designed to avoid the word count limit for petitions set forth in our rules.”). Additionally, Petitioner refers to “Examiner” over twenty times where proper grammar would require referring to “the Examiner.”

Even with such gamesmanship, Petitioner could not meet the word count limits, and actual intent to circumvent the 14,000 word limit can be inferred from Petitioner’s use of improper citation formats, improper incorporation by reference of its expert’s declaration, and repeated pattern of violations in this and at least twelve other matters filed by Petitioner. The Petition should not be considered. *See Patent Trial and Appeal Board Consolidated Trial Practice Guide*, November 2019 at 40 (“Parties should not abuse the process. Excessive words in figures, drawings, or images, deleting spacing between words, or using excessive acronyms or abbreviations for word phrases, in order to circumvent the rules on word count, may lead to a party’s brief not being considered.”) (citation omitted).

Worse yet, Petitioner’s claim chart cites improperly incorporates by reference over 180 paragraphs from its expert’s declaration (Ex. 1004) without

explanation. *See Cisco Sys., Inc. v. C-Cation Techs., LLC*, IPR2014-00454, Paper 12 at 8 (P.T.A.B. Aug. 29, 2014) (informative); 37 C.F.R. § 42.6(a)(3). Every row of Petitioner's claim chart ends with a naked citation to swaths of paragraphs from its expert's declaration. *See* Pet. at 37–65 (claim charts citing 186 paragraphs from Ex. 1004, yet relying on only 22 of them in any arguably meaningful way). Petitioner has violated the rule against incorporation by reference, and the incorporated material should either not be considered or be considered further evidence of Petitioner's word count violations. *See Limelight Networks, Inc. v. Akamai Techs., Inc.*, IPR2016-01894, Paper 8 at 16 (P.T.A.B. Mar. 8, 2017) (declining to consider arguments incorporated by reference into a petition “made only in a supporting document” and indicating that such gamesmanship could also violate the word count rule).

The Board has the authority and discretion to “dismiss a petition or fashion a less severe remedy” for abuses of the rules and word count. 37 C.F.R. §§ 42.5, 42.12(b)(8); *Panduit Corp. v. Corning Optical Commc'ns LLC*, IPR2017-00528, Paper 7 at 20 n.3 (P.T.A.B. May 30, 2017) (“Parties and their counsel ought to give strict attention to the related rule especially as it requires an attorney certification.”); *Innovations4Flooring NV v. Välinge Innovation AB*, IPR2017-02130, Paper 8 at 4 (P.T.A.B. Feb. 7, 2018); *Google Inc. v. Ji-Soo Lee*, IPR2016-00022, Paper 25 at 5 (P.T.A.B. Nov. 23, 2016). Petitioner's flagrant and repeated

violation of the rules spanning over a dozen of its recently-filed petitions warrants discretionary denial to discourage repeated rule violations.

III. THE '266 PATENT

A. Overview

The '266 Patent is directed to “protecting a secured network.” Ex. 1001 at Abstract, 1:59–60. Figure 1 shows a network environment having packet security gateways (“PSGs”) protecting networks A–D. *Id.* at 4:40–60, 5:12–22, FIG. 1.

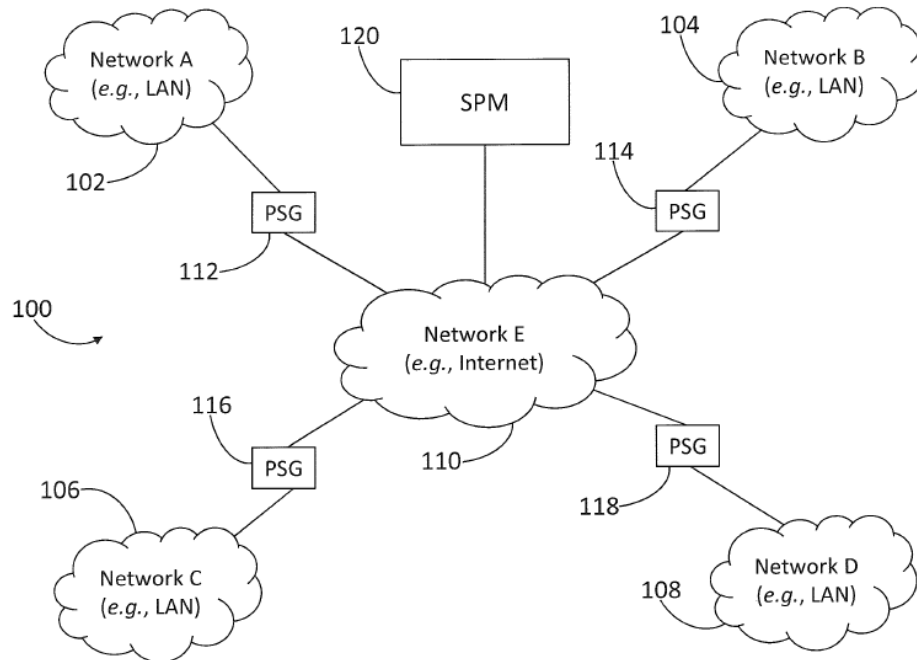


FIG. 1

Ex. 1001, FIG. 1.

A PSG receives packets and proactively protects a network from malicious attacks based on dynamic security policies. *Id.* at 4:61–5:11, 5:35–53, 11:22–33, 14:9–39, 19:38–41, FIGS. 1, 9. A dynamic security policy includes rules that “specify criteria and one or more packet transformation functions that should be

performed for packets associated with the specified criteria.” *Id.* at 5:4–9, 7:23–

26. Transformation functions include forwarding or dropping packets. *Id.* at 2:19–28, 3:4–14.

Because “the path a given packet may take cannot be readily predicted,” PSGs are placed at each boundary between a protected network and an unprotected (*e.g.* Network E). *Id.* at 5:23–34, 3:54–58, FIG. 1. For example, Figure 7 illustrates several protected networks, each having multiple boundaries with an unprotected network, such as the Internet. *Id.* at 16:44–48, 16:62–17:1, FIG. 7. PSGs are “located at each boundary between network A 702 and network C 706, and each boundary between network B 704 and network C 706.” *Id.* at 16:62–65, FIG. 7.

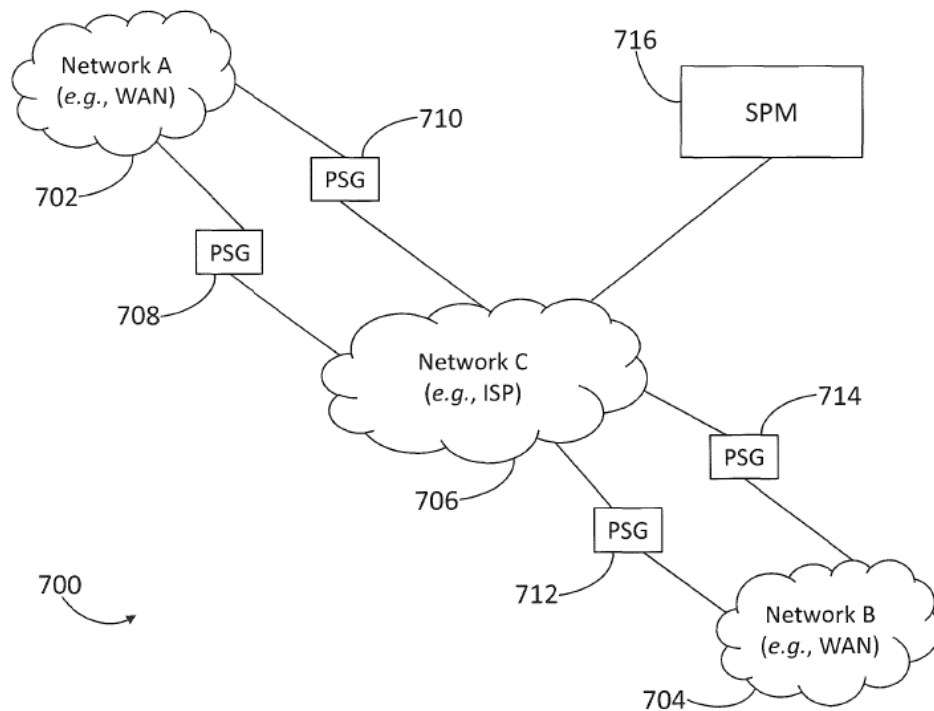


FIG. 7

Ex. 1001, FIG. 7.

Each PSG receives and filters packets that originate from outside a protected network that are destined for a host within the protected network, and also receive and filter packets that originate from inside the protected network and that are destined for another network. *Id.* at 3:44–53, 7:7–19. This arrangement enables a PSG to filter and perform transformation functions on all packets traversing the boundary in either direction, thus protecting the network (e.g., network A) “from malicious network traffic” and preventing “malicious traffic from leaving” the protected network. *Id.* at 7:17–19.

B. Prosecution History

The '266 Patent is the fifth patent in a series of continuations. Ex. 1001, code [63].¹ The Examiner of the '266 Patent also examined the parent '437 Patent. *Id.* at 1; Ex. 2008 at 1. The Examiner allowed the claims of the '437 Patent over *Jungck* based on added limitations requiring, among other things: “a plurality of packet security gateways that collectively provide an entire interface across a boundary” of a protected network and “packet filtering rules to be applied to all network traffic traversing the boundary.” Ex. 2008 at 150–53, 157–60, 164–67, 254, 256, 259, 289–91.

Originally filed independent claims 1, 8, and 15 of the '266 Patent included limitations substantially similar to the “entire interface” and “all traffic” limitations in the '437 Patent that the Examiner previously determined were missing in the prior art. Ex. 1002 at 42–47; Ex. 2008 at 289–91. Given that the Examiner already determined that *Jungck* did not disclose these claim elements, he did not reapply *Jungck* to those elements the pending claims. Instead, the Examiner

¹ Continuation of U.S. Patent No. 10,567,437 (Ex. 2007), which is a continuation of U.S. Patent No. 10,091,246 (Ex. 2013), which is a continuation of the '077 Patent (Ex. 1005), which is a continuation of the '205 Patent (Ex. 1006).

rejected the independent claims as allegedly obvious over two other references:

Jalava (Ex. 2009) in view of *Bhatnagar* (Ex. 2012).² Ex. 1002 at 148–62, 164–77.

Some dependent claims were rejected based on a combination of *Jalava*, *Bhatnagar*, and *Jungck* (Ex. 1051).

The Examiner then allowed the claims after Patent Owner amended the claims and further distinguished these references. *Id.* at 307–14, 333–45. Specifically, the claims were amended to specify that: (1) the “packet filtering rules” “comprise packet matching criteria corresponding to one or more network addresses” and are automatically created or altered by the security policy management server (“SPMS”) based on “aggregated” malicious traffic information; and (2) that the “aggregated malicious traffic information” is both (a) received from “at least one third party” malicious host tracker service “located in the one or more networks other than the network protected by the packet security gateway” and (b) “comprises network addresses that have been determined, by the

² *Bhatnager* does not disclose these claim elements because it only discloses a single firewall at the network boundary rather than “a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network,” as claimed. Ex. 1001, Claim 1.

at least one third party malicious host tracker service, to be associated with malicious network traffic.” *Id.*

IV. CLAIM CONSTRUCTION

Petitioner has proposed the Board adopt several claim constructions from prior proceedings. Pet. at 18–21. These constructions were determined under the broadest reasonable interpretation standard and do not apply to these proceedings as a matter of course.

The preambles of independent claims 1, 8, and 15 should be treated as limiting. These preambles provide antecedent basis for “packet security gateway,” “boundary,” “network,” and “one or more other networks.” Ex. 1001 at 20:64–21:2, 22:13–18, 23:35–42. The preambles also recite the “plurality of packet security gateways that collectively provide an entire interface across a boundary of a [protected] network,” which is “essential to understand” the “all traffic” limitation in the body of these claims and thus ““give life, meaning, and vitality”” to the claims. *Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (citation omitted). The preambles provide the context for the body of the independent claims by defining the arrangement of the “plurality of packet security gateways” relative to the “boundary” of the protected network and thus the basis for applying “packet filtering rules . . . to all network traffic traversing the boundary.” *See, e.g.*, Ex. 1001 at 20:64–21:8. The “entire interface”

limitation also was relied on during prosecution of the parent '437 Patent's claims to distinguish them from the prior art. *See* Ex. 2008 at 254–61; *see also Catalina*, 289 F.3d at 808–09. Petitioner does not dispute the preambles are limiting. Pet. at 18–21, 37.

Otherwise, at this preliminary stage, no express construction of any other term is needed to resolve any controversy here. *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (citation omitted). Patent Owner does not waive any rights to assert constructions should trial be instituted.

V. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 325(d)

The Board should deny institution under 35 U.S.C. § 325(d) because the Petition re-uses the same art and arguments that was previously presented to the Patent Office. 35 U.S.C. § 325(d) (“In determining whether to institute or order a proceeding . . . the Director may take into account whether, and reject the petition or request because, the same or substantially the same prior art or arguments previously were presented to the Office.”).

The Board applies a two-part framework in evaluating the prior consideration of the same or substantially the same prior art or arguments. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 7–9 (P.T.A.B. Feb. 13, 2020) (precedential) (describing a two-part framework that demonstrates “a commitment to defer to previous Office

evaluations of the evidence of record unless material error is shown”). First, the Board considers whether the same or substantially the same prior art or arguments previously were presented to the Patent Office. *Id.* at 7–8. If this condition is satisfied, the Board then considers whether the petitioner has demonstrated a material error by the Patent Office in the patentability of the Challenged Claims. *Id.* at 8–9.

The first prong of *Advanced Bionics* is satisfied here. The Patent Office during the prosecution of the '266 Patent application considered *Jungck*, related IPR proceedings referencing *Jungck*, as well as substantially the same art as the Petition's secondary references. *See* Ex. 1002 at 187–95, 316–21. Not only did the Patent Office consider related IPR proceedings, which referenced *Jungck*, but it also issued a rejection applying *Jungck*. Under *Advanced Bionics* Second Prong, Petitioner fails to show that there was a material error by the Patent Office in its consideration of *Jungck*, the same art presented here. Therefore, the Board should exercise its discretion under § 325(d) to deny this Petition.

A. The Same or Substantially the Same Art and Arguments Were Previously Presented to the Office

1. The Office Already Determined that *Jungck* Does Not Disclose the “Entire Boundary” and “All Traffic” Limitations

Petitioner admits that the Office already considered *Jungck* with respect to the Challenged Claims. Pet. at 9. Petitioner fails to inform the Board, however,

that, the Examiner was intimately familiar with *Jungck*, having already determined that it does not disclose the “entire boundary” and “all traffic” limitations during prosecution of the related '437 Patent.

The '266 Patent is a direct continuation of the '437 Patent. Ex. 1001, code [63]. The same Examiner examined both patents. Ex. 1002 at 146; Ex. 2008 at 135–36. During prosecution of the '437 Patent, *Jungck* was expressly considered, repeatedly discussed, and overcome. Ex. 2007, code [56]; Ex. 2008 at 102–03, 151, 180, 226, 244, 263, 290–91. For example, the Examiner explicitly determined that *Jungck* fails to disclose the same “entire boundary” and “all traffic” limitations also recited in Independent Claims 1, 8, and 15 of the '266 Patent. Ex. 2008 at 291.

Thus, the Office has considered the exact same prior art and arguments that Petitioner advances in this case without even acknowledging the Office's prior consideration of *Jungck*. See Pet. at 9–13. Petitioner's silence on this point is inexcusable because it has also filed a petition challenging the validity of the '437 Patent in IPR2021-01153 (Ex. 2016) where it discussed that patent's prosecution history. See Ex. 2016 at 8–12.

Beyond the fact that the Examiner had already determined that *Jungck* does not disclose the “entire boundary” and “all traffic” elements, the Examiner also applied to *Jungck* to pending claims of the '266 Patent where the Patent Owner

once again distinguished the reference. Ex. 1001, code [56]; Ex. 1002 at 99, 187–95, 262. It is no surprise that *Jungck* was extensively considered during prosecution of the '266 Patent given that the Examiner was already well-versed in the references' teachings and because the Examiner had a duty to consider the references in the immediate parent application. Manual of Patent Examining Procedure ("MPEP") §§ 609.02, 2001.06(b) (9th ed. Rev. 10.2019, June 2020).

While Petitioner alleges that a pair of prior Board decisions regarding the '205 Patent (IPR2018-01443, -01444) and their summary affirmance were not "properly" considered (Pet. at 9–10), those decisions, which do not contain any discussion of the "entire boundary" or "all traffic" limitations, were presented to the Office and were expressly considered by the Examiner along with their respective petitions and expert declarations. Ex. 1002 at 202, 293. *Advanced Bionics* Factor 1 is met for *Jungck* and the arguments from the prior proceedings.

2. *Jungck's "Virus Watch Service"*³ is Substantially Similar to and Cumulative of *Bhatnagar*

Petitioner relies on *Jungck's* disclosure of a "virus watch service" that "monitor[s] . . . for malicious [] code" to show the claimed "third party malicious host tracker service" that provides the "aggregated malicious traffic information" ([1.c]). See Pet. at 47–54 (citing Ex. 1051, ¶ [0111]) (further citations omitted). Even though the record is clear that the Examiner thoroughly considered all aspects of *Jungck*—which would have included *Jungck's* "virus watch service"—this aspect of *Jungck* is also cumulative to *Bhatnagar*, which the Examiner applied during prosecution of the '266 Patent. Ex. 1002 at 154. The Challenged Claims notably differ from the claims of the '205 Patent because they require a "third party malicious host tracker service" rather than the broader "subscription service that aggregates information associated with malicious network traffic" recited in the '205 Patent.

³ The Claims of the '205 Patent found unpatentable in IPR2018-01443 (Ex. 2014) refer broadly to a "subscription service that aggregates information associated with malicious network traffic" and do not mention a "malicious host tracker service." See, e.g., Ex. 1006, Claim 14.

During prosecution of the '266 Patent, the Examiner cited *Bhatnagar*'s disclosure of "continually updating . . . detection points 28 in real time as threats are discovered . . . to immunize the network against outbreaks of malicious code" for this limitation. *Id.* (citing Ex. 2012, ¶ [0024]); Ex. 2012 at Abstract, ¶¶ [0006], [0022] (describing a "security service" that "obtain[s] the signature of a threat" from "security agents" "that are designed to detect new viruses and other types of malicious code"). In response, Patent Owner observed that "*Bhatnagar* teaches '*malicious traffic information*' through its patterns; that is, '*malicious code definitions*'" rather than "network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic." Ex. 1002 at 319. Accordingly, *Jungck* is cumulative to *Bhatnagager* because *Jungck*'s "virus watch service" also "monitor[s] the data transmission being generated by clients 102, 104, 106, 602 for ***malicious program code***." Ex. 1051, ¶ [0111]; *Universal Imaging Indus., LLC v. Lexmark Int'l, Inc.*, IPR2019-01383, Paper 7 at 16 (P.T.A.B. Feb. 27, 2020) (reference is cumulative of art involved in prosecution where "there is no material difference" between the two).

3. The Patent Office Previously Considered Substantially the Same Art as *Wood* and *Sarathy*.

Likely because Petitioner recognized that *Jungck* does not disclose the malicious host tracker service claim elements and that the claims of the '266 Patent

are materially different from those of the '205 Patent, it introduces two new references, *Wood* and *Sarathy*. See, e.g., Pet. at 33–36 (arguing it would be obvious to combine *Jungck* and *Wood*); *id.* at 65–67 (arguing that it would be obvious to combine *Jungck* and *Wood* with *Sarathy*). However, *Wood* and *Sarathy* are substantially the same as the art previously considered by the Examiner. Where, as is the case here, Petitioner “relies on [a reference] in the same manner” as the reference previously presented to the Office during prosecution, discretionary denial is appropriate. *Advanced Bionics*, Paper 6 at 19.

First, Petitioner admits that *Wood* and *Sarathy* are cumulative of *Jungck*, alleging that both teach the same limitations and have similar goals. Pet. at 36 (both have the same goal of real time network protection from malware); *id.* at 47–51, 55–58 (both allegedly teach “aggregated malicious traffic information” in [1.c], “updated malicious traffic information” in [1.e]). Compare Pet. at 31–36 with *id.* at 65–67 (alleging both *Jungck* and *Sarathy* disclose “a security policy management server external from the network protected by the packet security gateway” in [1.a]). At most, Petitioner makes a generic allegation of some added “implementation” detail in *Wood* and *Sarathy* (Pet. at 35, 65), but never explains what disclosure is alleged to be missing from *Jungck*, how *Wood* and *Sarathy* address the deficiency, or why *Wood* and *Sarathy* are not cumulative to the references considered during prosecution. See Pet. at 51–52, 57, 59–61, 65–67.

Wood alleged disclosure of “information provided by a third-party virus watch service” (Pet. at 2) is cumulative to disclosures in the art the Examiner considered during prosecution of the '266 Patent., specifically *Bhatnagar et al.* (Ex. 2012, “*Bhatnagar*”) and Van Der Merwe et al. (Ex. 2015, “*Van Der Mere*”). See, e.g., Ex. 1002 at 186–87 (“It would have been obvious to one of ordinary skill in the art, having the teachings of Jalava, Bhatnagar, and Van Der Merwe before him or her, to modify [those references] with the teachings of Van Der Merwe to include *wherein the malicious traffic information comprises a list of network addresses known to be associated with malicious network traffic* as claimed because Jalava's system and method provides a management server that remotely connects to firewalls/gateways at protected networks to provide packet filtering rules and updates.”).

Petitioner's reliance on *Sarathy* for its alleged disclosure of a security management server external from the protected network also closely resembles art previously considered by the Examiner. See Pet. at 65–67. Particularly, the Examiner considered *Jalava* that discloses a management server that is external to the protected network. See, e.g., Ex. 1002 at 150. Thus, Petitioner relies on *Sarathy* in the same manner as *Jalava*, which, as the Examiner concluded, did not taken alone or in combination render obvious the claimed invention. See *id.* at 339, 345.

Thus, Petitioner relies on the combination of *Jungck*, *Wood*, and *Sarathy* in the same manner as the *Jalava-Bhatnagar-Van Der Mere* combination, which, the Examiner ultimately concluded, did not render the claimed invention obvious. See *id.* at 333–45 (allowing the Challenged Claims because the combination failed to teach an SPMS automatically creating or altering packet filtering rules based on aggregated malicious traffic information or updating those packet filtering rules based on updated malicious traffic information). Critically, Petitioner does not rely on *Wood* or *Sarathy* as allegedly disclosing an SPMS that automatically creates or alters packet filtering rules based on aggregated malicious traffic information. See *Pet.* at 47–54 (relying only on *Jungck* as allegedly teaching this aspect of the Challenged Claims).

Given that the Patent Office during prosecution of the '266 Patent application previously considered *Jungck* and substantially the same prior art and arguments as those raised in the instant Petition, the first prong of the *Advanced Bionics* framework is thus satisfied.

B. Petitioner Does Not Show that the Patent Office Materially Erred

“If a condition in the first part of the framework is satisfied and the petitioner fails to make a showing of material error, the Director generally will exercise discretion not to institute” *Advanced Bionics*, Paper 6 at 8–9. Despite overwhelming evidence that Petitioner presents the same art and

arguments already presented and expressly considered during prosecution, Petitioner alleges the Examiner erred based on supposedly contradictory findings on *Jungck* in the 1443 and 1444 FWDs. Pet. at 9–13. Petitioner is wrong.

1. Petitioner Does Not Acknowledge the Office's Prior Consideration of *Jungck* With Respect to the "Entire Interface" and "All Traffic" Limitations

First, the Petition should be denied because Petitioner fails to allege material error in the Office's prior consideration of *Jungck* with respect to the "entire interface" and "all traffic" limitations. Incredibly, not only does Petitioner not mention these limitations in its § 325(d) analysis, it did not even apprise the Board of the existence of the '437 Patent or inform the Board that the Office already decided this precise issue. See Ex. 2008 at 291. In this light, Petitioner's argument that the Examiner erred by failing "to apply *Jungck* to any independent claim" is particularly disingenuous. It is plain that the Examiner did not apply *Jungck* to the "entire boundary" and "all traffic" limitations of the '266 Patent because he already determined that *Jungck* does not disclose those limitations. There can be no question, therefore, that the Office already decided this very issue or that Petitioner failed even to allege material error. The Board should exercise its discretion to deny institution under § 325(d) for this reason alone.

Second, Petitioner alleges that the Examiner erred by failing to explain how the allowed claims overcame the prior art and arguments analyzed in the

1443/1444 FWDs. However, because the '205 Patent does not include the “entire interface” and “all traffic” limitations, the Board made no findings in those proceedings that the Examiner could have overlooked. Petitioner fails even to point to a single aspect of the FWDs that is relevant to these limitations, leaving it up to the Board to identify some potential error on the basis that a related but materially different patent was found unpatentable. *See Mercedes-Benz USA, LLC v. Stragent, LLC*, IPR2021-00426, Paper 13 at 18 (P.T.A.B. July 19, 2021) (denying institution under § 325(d) after determining the petitioner had “relied heavily on the Board’s previous determination about a related patent with different subject matter than that recited [by the Challenged Claims]”).

Thus, Petitioner’s bare allegation that the “Examiner made findings that contradicted the Board’s findings in the 1443/1444 FWDs” regarding an SPMS automatically creating or altering packet filtering rules based on aggregated malicious traffic information (he did not) does not address, let alone demonstrate, material error in the Office’s earlier determination that *Jungck* does not disclose the “entire interface” and “all traffic” limitations.

The Office has considered the exact same prior art and arguments that Petitioner advances in this case, and Petitioner has made no effort whatsoever to acknowledge those findings or even allege error. *See* Pet. at 9–13. The Board should deny institution on this basis alone. *Advanced Bionics*, Paper 6 at 8–9 (“If a

condition in the first part of the framework is satisfied and the petitioner fails to make a showing of material error, the Director generally will exercise discretion not to institute *inter partes* review.”).

2. Petitioner Does Not Demonstrate Material Error in the Examiner's Consideration of *Jungck* Regarding the Malicious Host Tracker Elements

Petitioner also fails to demonstrate material error in the Examiner's determination that *Jungck* does not teach SPMS that “automatically create[s] or alter[s]” packet filtering rules based on receiving, from “at least one third party malicious host tracking service” external to the protected network, “aggregated malicious traffic information” comprising “network addresses . . . determined, by the . . . third party malicious host tracker service[s], to be associated with malicious network traffic.” Ex. 1002 at 333–37; Ex. 2008 at 290–91; §§ VI.A–C, *infra*.

Petitioner alleges the Examiner materially erred by not following the Board's prior determination that in the 1443 FWD where the Board addressed whether *Jungck* discloses four limitations: (1) “at each packet security gateway of one or more packet security gateways associated with a security policy management server,” (2) “receiving a plurality of dynamic security policies from the security policy management server, wherein receiving the plurality of dynamic security policies comprises,” and (3) “the SPMS [] receiving from a subscription service that aggregates malicious network traffic information, a list of network

addresses known to be associated with malicious network traffic,” and (4) “the SPMS generating, based at least in part on the list, one or more rules included in the plurality of dynamic security policies.” Pet. at 12 (citing Ex. 1014 at 11, 16–17, 46–48).

Even a cursory comparison, however, shows these limitations that led to allowance of the '266 Patent are different from any limitations considered during the IPR of the '205 Patent. For example, the claims in the prior proceeding did not require “automatically creating or altering rules” by the SPMS based on aggregated malicious traffic information from outside the protected network. Instead, the rule only needed to be “generated” by the SPMS. Ex. 1006 at 22:19–27 (claim 14), 24:49–56 (claim 30); 27:25–33 (claim 46). Additionally, the cited portions of the 1443 FWD address receiving “dynamic security policies” from the SPMS, not packet filtering rules. Ex. 1014 at 6–8. The Board’s prior construction held that “dynamic security policies” are broader than just rules, but includes “any rule, message, instruction, file, data structure, or the like that specifies criteria corresponding to one or more packets and identifies a packet transformation function to be performed on packets corresponding to the specified criteria.” *Id.* (also construing a “rule” to mean “a condition or set of conditions that when satisfied causes a specific function to occur”).

Moreover, the Examiner also determined the prior art did not disclose “updat[ing]” these automatically created or altered SPMS packet filtering rules “based on updated malicious traffic information received from the . . . third party malicious host tracker service.” Ex. 1002 at 333–37. Petitioner again alleges the Board found that *Jungck* teaches “rules are dynamically modifiable/resettable based on malicious network traffic information received from a third-party virus watch service.” Pet. at 13. But, as just explained, Petitioner ignores that a dynamic security policy and a rule are different and that the Board never addressed whether *Jungck* discloses “automatically creat[ing] or alter[ing]” rules by the SPMS based on aggregated malicious traffic information from outside the protected network.

Moreover, the underlying allegations were also different. In the prior proceeding, Petitioner alleged that the subscribing server was the SPMS. Ex. 1014 at 13. While Petitioner ostensibly repeats that position in a footnote in the background (Pet. at 22, n.10), Petitioner’s new allegation here is that an external management device or external device 724 is now the SPMS. See Pet. at 25–26, 42 (“other remote server”);⁴ *id.* at 47–48 (same); *id.* at 55–56 (same); *id.* at 59

⁴ Petitioner never explains or supports its allegation that there is another “remote server” in *Jungck*.

("external devices"). Petitioner does not try to reconcile these inconsistent positions or attempt to explain how the Board's prior decisions regarding a different mapping of *Jungck*'s teachings to different claim elements somehow control the outcome in this case.

Petitioner's attempts to manufacture error with reference solely to prior decisions of the Board that did not address the same limitations found patentable over *Jungck* during prosecution of the '266 and '437 Patents should be rejected. At the very least because "reasonable minds can disagree regarding the purported treatment" of *Jungck* in the earlier FWDs, "it cannot be said that the Office erred in a manner material to patentability." *Advanced Bionics*, Paper 6 at 9. The Petition should be denied.

VI. THE CHALLENGED CLAIMS ARE PATENTABLE

As a preliminary matter, collateral estoppel cannot bar Centripetal's argument. The standard for finding collateral estoppel is strict and requires the identical issues to be decided in the first action:

[1] that in the prior action the party against whom estoppel is sought had a full and fair opportunity to litigate the issue; [2] the issue was actually litigated; [3] the controlling facts and applicable legal rules were the same in both actions; [4] resolution of the particular issue was essential to the final judgment in the first action; and [5] the identical issue was decided in the first action.

Comair Rotron, Inc. v. Nippon Densan Corp., 49 F.3d 1535, 1537 (Fed. Cir. 1995) (citations omitted). No prior Board proceeding determined that any of the art asserted in this case discloses the “entire interface,” “all traffic,” “automatic rules,” or “updated rules” limitations, so there can be no collateral estoppel. To the contrary, the Office already considered and rejected the same or substantially similar art and arguments with respect to these limitations. *See* § V, *supra*.

A. *Jungck* Does Not Disclose the “Entire Interface” or “All Traffic” Limitations

Independent Claims 1, 8, and 15 each recite two limitations that the Examiner previously identified as missing from *Jungck* during prosecution of the parent '437 Patent and which were not recited in the claims of the prior '205 and '077 Patents:

- “a plurality of packet security gateways that collectively provide an entire interface across a boundary” of a protected network; and
- “packet filtering rules to be applied to all network traffic traversing the boundary.”

See Ex. 2008 at 151–52, 244, 253–54, 262, 290–91. Petitioner relies only on *Jungck*'s edge servers (the alleged PSGs) to meet the “entire interface” limitation. Pet. at 37–39 ([1.pre]). Petitioner relies only on the rules applied by *Jungck*'s edge servers to allegedly show the claimed “packet filtering rules” that are applied to “all network traffic traversing” *Jungck*'s POPs (the asserted “boundary”). *Id.*

at 42–43. Petitioner's obviousness grounds disregard the role of *Jungck*'s edge caches, which are located in network paths that bypass the edge servers entirely.

Petitioner goes out of its way to avoid even mentioning these edge caches, repeatedly excising any mention of the edge caches from its quotations from *Jungck*. This pattern of omissions repeats throughout the petition. *Id.* at 22–23, 37–38, 40–42, 44, 62. For example, for the collective “entire interface” limitation, Petitioner quotes *Jungck* ¶ [0107], but misleadingly omits mention of the edge caches using ellipses and partial quotations (omitted material underlined):

Further, service providers 118, 120 each include an edge server 602A, 602B **and an edge cache 604A, 604B coupled with the routing equipment 206 of the service providers 118, 120 so as to be able to** intercept all network traffic flowing between the POP's 114, 116 and the network 100.

Pet. at 37.

An edge server 602 **and edge cache 604** “may be provided at ...” **every service provider 118, 120 or at** every major network 100 intersection so as to provide coverage of every POP 114, 116 on the edge 124 of the network 100, **i.e. to minimize the size of the sub-network downstream from the edge server 602.**

Id. at 22–23. Petitioner similarly omits reference to *Jungck*'s edge caches when quoting from *Jungck*'s paragraph 116:

[T]he network of edge servers **and edge caches** located at every

major network intersection so as to cover every POP, thereby minimizing the size of the sub-network downstream from the edge server, forms a security barrier which isolates the core infrastructure and servers of the network/internet from the edge where the clients are located.

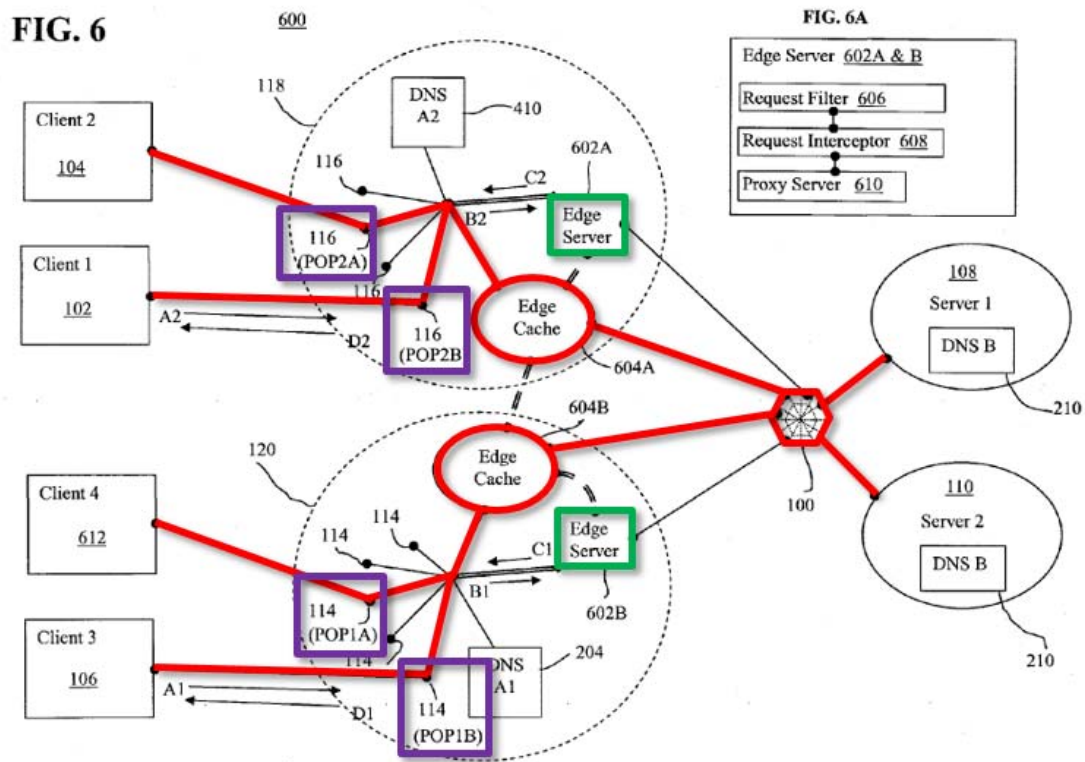
Id. at 41. Petitioner omits mention of the edge caches for good reason: The edge caches contradict Petitioner's position that *Jungck*'s edge servers "intercept all network traffic" between the POPs and provide the "security barrier" around *Jungck*'s network that "isolates the core infrastructure and servers of the network." *Id.* at 37–38 (citing Ex. 1051, ¶¶ [0107], [0116]). This omission is fatal to the Petition.

1. *Jungck* Fails to Disclose the "Entire Interface" Limitation

Independent claims 1, 8, and 15 require a "plurality of packet security gateways that collectively provide an entire interface across a boundary of a network." Petitioner identifies *Jungck*'s POPs as the alleged "boundary" and asserts that the edge servers "are located at" the POPs. Pet. at 22; *id.* at 37–38. However, *Jungck* describes network paths across the alleged "boundary" that bypass *Jungck*'s edge servers, demonstrating that the edge servers do not form the "entire interface" across the alleged boundary.

As shown below in annotated Figure 6, network paths (red) exist between *Jungck*'s clients 102–106 and 612, POPs 114 and 116 (purple), routing equipment

(206 in FIG. 5), edge caches 604A–B, network 100, and servers 108, 110—all of which bypass *Jungck*'s edge servers (**green**). Ex. 1051, ¶ [0107] (“edge cache 604A, 604B coupled with the routing equipment 206”); *In re Meng*, 492 F.2d 843, 847 (C.C.P.A. 1974) (“[A] drawing is available as a reference for all that it teaches a person of ordinary skill in the art.”).



Ex. 1051, FIG. 6 (annotated). Petitioner’s argument that *Jungck*’s edge servers (the asserted “packet security gateways”) provide the “entire interface” across *Jungck*’s POPs (the asserted “boundary”) fails in view of these network paths that cross the POPs while bypassing those edge servers. Pet. at 37–46 ([1.pre]–[1.a]).

There are many circumstances in which traffic bypasses the edge servers via

the edge caches. For example, after a client request content from server 108, the edge server translates server 108's domain name into the IP address of the edge cache so that the client communicates directly with the edge cache instead of either the edge server or server 108. Ex. 1051, ¶¶ [0095] (describing how clients make content request directly to the edge cache), [0111] (same for the third embodiment). Similarly, in the event that there is a cache miss, the edge cache “makes its own request for the uncached content from the server 108,” bypassing the edge server. Ex. 1051, ¶¶ [0096], [0112]. Finally, the edge caches send traffic carrying cached content along the same network paths back to the client, again bypassing the edge server. Ex. 1051, ¶ [0109], FIG. 6.

Ignoring these express teachings, Petitioner represents that *Jungck* teaches that its edge servers “intercept all network traffic flowing between the POP's 114, 116 and the network 100” and that “isolate[] the core infrastructure and servers of the network . . . from the edge where the clients are located.” Pet. at 37–38 (citing Ex. 1051, ¶¶ [0107], [0116]). This is demonstrably false. Petitioner misleadingly edits out all mention of the edge caches from these paragraphs to avoid the inconvenient truth that the edge servers do not intercept all network traffic and isolate the network alone.

As both paragraphs cited by Petitioner make clear, the edge cache is needed for both interception of traffic and to isolate the network. Ex. 1051, ¶¶ [0107]

(“edge server 602A, 602B **and an edge cache 604A, 604B** coupled with the routing equipment 206 of the service providers 118, 120 **so as to be able to intercept all network traffic** flowing between the POP's 114, 116 and the network 100”), [0116] (“Further the network of edge servers **and edge caches** located at every major network intersection so as to cover every POP....) (emphasis added). *In re Wesslau*, 353 F.2d 238, 241 (C.C.P.A. 1965) (Petitioner cannot just “pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests . . .”).

Petitioner also addresses two alternative interpretations of the claims: assuming the claims require (1) “multiple edge servers” or (2) “multiple POPs each having at least one edge server”—neither of which is a claim limitation and appears to read *Jungck*'s edge servers and POPs into the claims. Pet. at 39. As to the “multiple edge servers,” Petitioner relies on *Jungck*'s disclosure of hierarchical edge servers to prevent overload “renders obvious multiple PSGs collectively provide **an interface** across a single boundary,” but that analysis does not address how the PSGs “**collectively** provide an **entire** interface” across a single boundary or address *Jungck*'s edge caches. *Id.*

As to “multiple POPs each having at least one edge server,” that arrangement does not suggest that the edge servers for any one of those POPs

provide the “entire interface” across the POP. While Petitioner also argues that a skilled artisan “would have recognized the benefit of protecting a LAN with multiple devices in a LAN with multiple entry points” “to advantageously provide a comprehensive security barrier,” Petitioner does not explain what it means by a “comprehensive security barrier.” *Id.* Nor does Petitioner allege or explain how using multiple devices to provide a “comprehensive security barrier” to a LAN with multiple entry points would have resulted in those devices providing an “entire interface across a boundary” of that LAN. Petitioner’s expert declaration also lacks any further explanation as it simply parrots the Petition. *Id.* at 37, 39 (citing Ex. 1004, ¶¶ 222–23). And even if *Jungck* did disclose multiple edge servers providing an interface across a single POP, such a disclosure would not eliminate *Jungck*’s edge caches, which as discussed above, provide a network path through *Jungck*’s POPs while avoiding its edge servers entirely.

Petitioner’s reliance on collateral estoppel for its arguments about a LAN with multiple entry points is also misplaced. *Id.* at 39 (citing Ex. 1012 at 40, n.8). The disputed issue in the prior proceedings was whether *Jungck* disclosed the “switching matrix” limitation. Ex. 1012 at 37–40. In that case, the Board accepted expert testimony “explain[ing] that a private LAN may have multiple entry points and, thus, multiple LAN switches, each with an associated edge server or packet interception device as described in *Jungck*.” *Id.* at 40. The Board did not face the

question of whether the “associated edge server(s)” in that context would have provided “an entire interface across a boundary” of that “private LAN” or determine that network paths through edge caches would not also exist in such embodiments.

As *Jungck*'s edge caches provide other network paths through the POPs that bypass the edge servers, Petitioner has not shown that *Jungck*'s edge servers “collectively provide an entire interface across” those POPs. Petitioner's obviousness ground thus fails to show *Jungck* discloses the “entire interface” limitation recited in Independent Claims 1, 8, and 15.

2. *Jungck* Does Not Disclose the All Traffic Limitation

(a) *Jungck*'s client requests do not traverse a boundary of a network protected by the packet security gateway.

First and foremost, *Jungck* fails to disclose “packet filtering rules to be applied to all network traffic traversing the boundary” because the client requests disclosed in *Jungck* never traverse the boundary at all.⁵ *Jungck*'s *raison d'être* is to isolate clients from subscribing servers such that “clients 102, 104 are prevented from any direct contact with server 108.” Ex. 1051, ¶ [0099]. Rather than

⁵ Petitioner identifies *Jungck*'s POPs as the alleged “boundary” and asserts that the edge servers “are located at” the POPs. Pet. at 21–22; *see also id.* at 33–34.

allowing any traffic from the client to traverse the boundary of the network allegedly protected by the edge servers, *Jungck* explicitly discloses that “it is the edge cache 508 and not the client 102, 104 which will request that content from the server 108.” *Id.*

Thus, while traffic from the clients reaches edge servers at the POPs, *Jungck*'s architecture explicitly and intentionally prevents all of that traffic from **traversing** this boundary into network 100. *See id.* at ¶ [0109] (“In this way, a comprehensive content delivery service is created which completely isolates the core 122 of the network 100 from untrusted and unregulated client 102, 104, 106, 602 generated network traffic.”). In fact, the **only** traffic that is allowed to traverse the network boundary is traffic that is not subjected to any packet filtering rules at all, *i.e.*, traffic not associated with a subscribing/affiliated server 108, 110. *Id.* at ¶ [0113] (“The request filter 606 first determines whether or not the traffic it is monitoring is associated with a subscribing/affiliated server 108, 110. If not, this traffic is ignored and allowed to proceed to its final destination.”). In all other cases, requests are “isolated” at the edge of network 100 and are not permitted to “traverse” the boundary. *See id.*, ¶ [0095] (requests are either satisfied by the edge cache, or the edge cache makes a request on behalf of the client).

Accordingly, *Jungck* by design fails to disclose “one or more packet filtering rules to be applied to all network traffic traversing the boundary.”

(b) *Jungck's edge caches bypass the edge servers and some traffic avoids the edge server's rules.*

Jungck also fails to disclose the claim limitation because, as discussed in detail above, *Jungck* discloses many types of traffic that bypass the edge servers and any packet filtering rules that they implement. *See* § VI.A.1, *supra*.

Petitioner relies exclusively on *Jungck's* edge servers applying rules to show the claimed “packet filtering rules” that are applied to “all network traffic traversing” *Jungck's* POPs. Pet. at 41–46 ([1.a]). But *Jungck* teaches network paths that bypass its edge servers when carrying network traffic through the POPs. Ex. 1051, FIG. 6. *Jungck's* edge servers redirect clients to request content from the edge caches or send content request packets to the edge caches for handling. *Id.*, ¶¶ [0095] (“[T]his effectively redirects the client 102, 104 to make all of its content requests from the edge cache”), [0113].⁶ If the cache server has the requested content, then the cache server serves the cached content to the requesting client. *Id.*, ¶¶ [0069], [0074], [0095] (“edge cache . . . attempt[s] to satisfy content requests from its cache storage”), [0109] (“requests will be redirected and served

⁶ *Jungck* explains that the edge servers and edge caches of its third embodiment operate similarly to those of its first and second embodiments. Ex. 1051, ¶¶ [0108]–[0109], [0113].

from the edge cache 604”), [0113].

Similarly, in the event that there is a cache miss, the edge cache “makes its own request for the uncached content from the server 108,” also bypassing the edge server. *Id.*, ¶¶ [0096], [0112]. Finally, the edge caches send traffic carrying cached content along those same network paths back to the client, bypassing the edge servers once again. *Id.*, ¶ [0109], FIG. 6.

Petitioner has not argued or shown that these content requests received by or the network traffic served by those edge caches would have been sent via anything but the network paths between *Jungck*’s clients and its edge caches. § VI.A.1, *supra* (annotated network paths in FIG. 6). Thus, Petitioner neither shows nor explains how *Jungck*’s cached content and redirected content requests across the boundary are subject to the edge server’s rules.

Given these disclosures, it is perhaps unsurprising that Petitioner’s analysis of the “all traffic” limitation is thin, amounting to a reference of an edge server that contains no mention of *Jungck*’s POPs. Pet. at 42. Petitioner first points to *Jungck*’s teachings that its edge servers temporarily divert packets to determine whether to take any action associated with a rule. *Id.* at 25. But Petitioner does not allege or show that the packets diverted by *Jungck*’s edge servers constitute “all traffic traversing” *Jungck*’s POPs. As previously discussed, no client requests that are subjected to alleged packet filtering rules traverse the network boundary,

and many types of traffic bypass *Jungck's* edge servers. Ex. 1051, ¶¶ [0069], [0070], [0076], [0109], [0113]. Petitioner simply ignores the existence of *Jungck's* edge caches and does not explain how that only passes through those edge caches, avoiding *Jungck's* edge servers, would be subject to any edge server rules.

Petitioner's deficient analysis of the "all traffic" limitation is also not saved by the brief mention of "ingress and egress filtering" and the use of "blocklists" by *Jungck's* fifth embodiment. Pet. at 43–44 (citing Ex. 1051, ¶ [0269]). That discussion never mentions any particular claim language, much less the "all network traffic traversing the boundary" language. *Id.* In fact, *Jungck's* fifth embodiment only filters packets within network 100, and not traversing any network boundary. *See, e.g.*, Ex. 1051, ¶¶ [0108], [0112], [0269], *id.*, FIGS. 9.

Petitioner also fails to provide any evidence to support its assertion that "applying filtering rules to all packets entering and leaving a network" was "well-known." *Id.* (citing Ex. 1051, ¶ [0269]). Petitioner cites paragraph 269 from *Jungck*, but paragraph 269 merely discusses filtering packets a single device ("device 900") that "intercept[s] and process[es]" all packets that the device happens to receive, not "all packets entering and leaving" *Jungck's* network as a whole. Ex. 1051, ¶¶ [0266], [0268]. Petitioner's claim chart does not explain why *Jungck's* limited teaching of intercepting and processing upstream and downstream packets in one device establishes that *Jungck's* "device 900" intercepts and

processes “all packets entering and leaving” that entire network or how and why that purported teaching would be used to modify the edge server/edge cache arrangement at the POPs.⁷

Finally, Petitioner cannot rely on collateral estoppel to show the “all traffic” limitation (Pet. at 37) because the claims at issue in the prior proceedings did not include the “all traffic” limitation. § VI, *supra*. Petitioner’s argument accounts for traffic in only one direction: traffic from *Jungck*’s clients to its servers. Petitioner argues that collateral estoppel applies to the PTAB’s finding that *Jungck* teaches “packet filtering rules to be applied at least to all traffic directed at servers on the network.” Pet. at 42 (citing Ex. 1014 at 13–18, 42, 49–50, 52–54; Ex. 1016 at 13–19, 42). Petitioner does not account for traffic travelling in the other direction, *i.e.* traffic that subscribing servers and edge caches send back to the requesting clients. Traffic through the POPs carrying cached content from *Jungck*’s edge caches back to the clients. As discussed in detail above, this traffic bypasses the edge server and is not subjected to the edge server’s rules. Ex. 1051, ¶¶ [0069], [0070], [0076], [0109], [0113]; § VI.A.1, *supra*. Thus, Petitioner’s collateral estoppel argument

⁷ Petitioner’s cited paragraphs from its expert declaration are no help as they provide just a summary of *Jungck*’s teachings about “device 900.” Pet. at 44 (citing Ex. 1004, ¶¶ 238–41).

cannot support a conclusion that *Jungck*'s edge servers apply rules to "all network traffic traversing" the alleged network boundary.

(c) *Jungck*'s edge server does not apply "one or more packet filtering rules" on to "all traffic traversing the boundary."

The '266 Patent describes and claims a packet security gateway applies packet filtering rules on packets traversing a boundary of a protected network and flowing to and from hosts located within the protected network. Ex. 1001, 7:3–19; *id.* at Claims 1, 8, and 15. For example, a PSG applies packet filtering rules on packets that, flowing in either direction, traversing the boundary of the network it protects in both directions. *Id.* at 7:14–19. In accordance with this disclosure, each independent claims requires that the packet security gateway apply one or more packet filtering rules on "all network traffic." *Id.*, Claims 1, 8, and 15.

Jungck's edge servers do not apply packet filtering rules to packets traversing the boundary that originate from the subscribing server (within the alleged protected network) and that are destined to a client (outside the alleged protected network). Cisco System, Inc.'s expert testified to this fact in a prior proceeding concerning *Jungck*'s applicability to U.S. Patent No. 9,560,077, acknowledging that the edge servers do not filter packets destined for *Jungck*'s clients because they are "not part of the networks that are being protected by the edge server." See Ex. 2011 (Second Jeffay Tr.) at 25:5–27:1; Ex. 2010 (First

Jeffay Tr.) at 44:7–16 (testifying that protecting a network means “trying to identify packets that match some specified criteria and dropping the packets”). Accordingly, *Jungck*’s edge servers/packet analyzer do not perform the recited packet filtering on traffic traversing the boundary and destined for clients because the edge servers do not protect those clients.

Petitioner’s reliance on *Jungck*’s fifth embodiment to support its conclusion that “POSITA would have understood that all packets entering or leaving the protected network would be compared against the blocklists” fails for several reasons. Pet. at 44. First, as Petitioner acknowledges, the network device of the fifth embodiment intercepts and processes packets from *within* network 100 rather than at a boundary of a protected network. Ex. 1051, ¶ [0268]; Pet. at 43 (acknowledging that device 100 is located within network 100 between “upstream network 100A and downstream network 100B”). Despite Petitioner’s acknowledgement that device 900 does not operate at the boundary of a protected network, it fails to explain why a POSITA would have been motivated to implement this type of filtering “to all packets entering and leaving a network” beyond its conclusory and unsupported allegation that such filtering was “well-known.” Pet. at 44; *see also* § VI.A.3, *infra* (discussing in detail the Petition’s lack of motivation to modify *Jungck*’s third and fifth embodiments to reach this claim element).

To the contrary, *Jungck*'s edge server only intercepts packets flowing in one direction, that of *Jungck*'s subscribing servers. See Ex. 1051, ¶¶ [0108]–[0113], [0120]–[0125]. The reason for this behavior that *Jungck*'s architecture is designed to intercept and filter packets close to the source before they enter the stream of Internet traffic, toward the subscribing servers. *Id.*, ¶ [0123] (“[I]t is optimal, in most Internet enhancement applications, to intercept and process packets ***close to their source before they enter the general stream of Internet traffic***....” (emphasis added)); see also *id.*, ¶ [0112] (the edge server performs ingress filtering on traffic that is destined to a subscribing server). Attempting to filter traffic after traversing network 100, as would be the case for traffic received from *Jungck*'s subscribing servers destined for the clients, directly contradicts to this principle, which explains why *Jungck* fails to disclose filtering such traffic whatsoever. See, e.g., *id.*, ¶ [0113] (returning requested content to the requesting client without applying any packet filtering rules).

Given the foregoing, Petitioner fails to establish that *Jungck* teaches or suggests applying one or more packet filtering rules to “all traffic” traversing the boundary of a protected network, including packets received from subscribing servers and destined for a client. Ex. 1001, Claims 1, 8, and 15.

3. Petitioner's Obviousness Grounds Do Not Adequately Explain Its Combinations, Including for the "All Traffic" and "Entire Interface" Limitations

Petitioner bears the burden to show "that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so." *Intell. Bio-Sys., Inc. v. Illumina Cambridge, Ltd.*, 821 F.3d 1359, 1367–68 (Fed. Cir. 2016) (citations omitted); *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). The Federal Circuit dictates that the Board must reject obviousness grounds that do not explain "how or why the references would be combined to arrive at the claimed invention." *See Metalcraft of Mayville, Inc. v. Toro Co.*, 848 F.3d 1358, 1367 (Fed. Cir. 2017) ("[W]e are left with only hindsight bias that *KSR* warns against.").

(a) Petitioner's generic motivations to combine *Jungck's* embodiments are conclusory and insufficiently specific to the claims.

Petitioner presents three generic reasons why a skilled artisan would have purportedly combined *Jungck's* three embodiments. Pet. at 31–33. None of Petitioner's motivations, however, identifies a reason why a skilled artisan would have modified any of *Jungck's* embodiments with any specific features to result in a particular claim limitation, including the "all traffic" and "entire interface" limitations that the Examiner highlighted as missing from the prior art. *Id.*;

Ex. 2008 at 291. Petitions devoid of citation or analysis to support its contentions are fatally flawed. *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-00582, Paper 34 at 28–30 (P.T.A.B. Aug. 5, 2019) (informative).

Petitioner's first and second reasons allege a skilled artisan would have combined *Jungck*'s third and fourth embodiments to decouple packet interception from packet processing or to provide a standardized interface to a network such as the Internet. Pet. at 31–33 (citing Ex. 1051, ¶ [0126]). Petitioner presents no more than what the purported results of its proposed motivations would have been: a “generic packet interception and pre-processing engine” or a “standardized interface to a network.” *Id.* at 32. This is not an explanation for how or “why” a skilled artisan would have been motivated to combine specific features from the embodiments let alone for any specific limitation of the claim.

Petitioner's third reason alleges a skilled artisan would have been motivated to combine *Jungck*'s third through fifth embodiments “to meet various design objectives such as adding network security devices without adding additional latency.” *Id.* at 33. Merely asserting “various design objectives” without explaining how or why a skilled artisan would have combined those embodiments to meet those objectives to arrive at the claimed invention does not meet Petitioner's burden. *Johns Manville Corp. v. Knauf Insulation, Inc.*, IPR2018-00827, Paper 9 at 13–14 (P.T.A.B. Oct. 16, 2018) (informative). It is unclear how

the fifth embodiment is even related here: Petitioner seems to rely on only *Jungck*'s third and fourth embodiments for avoiding additional latency. Pet. at 33 (“*Jungck* further describes Emb#4 as providing similar functions as Emb#3 ‘without introducing additional network latency’”) (citing Ex. 1051, ¶ [0126]). Petitioner identifies no other design objective for combining all three of *Jungck*'s embodiments. *Id.*

Petitioner's remaining motivation analysis is replete with conclusory and legally insufficient statements about similarity and predictable results. While Petitioner contends that *Jungck*'s fourth embodiment “provid[es] similar functions as” its third embodiment, Petitioner never identifies what those purportedly “similar functions” are. *Id.* Petitioner's argument that a skilled artisan would have “combine[d] features” of *Jungck*'s third through fifth embodiments “to yield predictable results” also fails to explain which specific features a skilled artisan would have combined and what the “predictable results” would have been. *Id.* Although Petitioner asserts that *Jungck*'s fifth embodiment “is directed to similar functionality and enhanced features to address higher traffic volume,” it never alleges that a skilled artisan would have been motivated to apply any particular teachings related to *Jungck*'s fifth embodiment to any other embodiment. *Id.* at 31–33. Indeed, Petitioner presents no clear reason for combining *Jungck*'s fifth embodiment with any other and vague insinuations of similarity are legally

insufficient for a rational to combine references.

Finally, the petition and expert declaration wind up its analysis of the generic motivations with only a conclusory remark about expectation of success with no corresponding analysis or explanation. *Id.* at 33 (citing Ex. 1004, ¶ 197). Petitioner's failure to explain how or why a skilled artisan would have reasonably expected success in combining *Jungck's* embodiments to achieve at least these two limitations is also grounds for denial. *Intell. Bio-Sys.*, 821 F.3d at 1367 ("The reasonable expectation of success requirement refers to the likelihood of success in combining references to meet the limitations of the claimed invention.").

As the Board has held, "that the [embodiments] have some common teachings is not sufficient to establish a reason to combine their teachings to achieve the method set forth in the claim." *Universal Imaging*, Paper 7 at 29, 31. "[I]t is not enough to show that 'a skilled artisan, once presented with the two references would have understood that they could be combined.'" *Pollard Banknote Ltd. v. Nanografix Corp.*, IPR2019-01288, Paper 10 at 14–15 (P.T.A.B. Jan. 8, 2020) (quoting *Pers. Web Techs. LLC v. Apple, Inc.*, 848 F.3d 848 F.3d 987, 993 (Fed. Cir. 2017)); *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015). Petition ignores these warnings, and has failed to explain how or why a skilled artisan would have combined *Jungck's* embodiments in the claimed manner with a reasonable expectation of success.

(b) Petitioner's motivations in the claim chart also have no meaningful connection to the claims, including the "entire interface" and "all traffic" limitations.

Petitioner's motivations do not mention any specific language of the challenged claims, and instead merely point back to its generic and legally insufficient motivations. Pet. at 31–33, 37–38 ([1.pre]), 41–44 ([1.a]), 46–47 ([1.b]), 47–50 ([1.c]), 55–56 ([1.e]).⁸ The Board has denied institution where a "Petitioner provides a discussion of motivation to combine that is unconnected to the claim limitations and Petitioner's claim mapping" and where that "Petitioner's claim mapping lacks sufficient explanation of how and why the prior art teachings would have been combined by a POSITA to arrive at the claimed invention." *PayPal, Inc. v. IOENGINE, LLC*, IPR2019-00930, Paper 16 at 27 (P.T.A.B. Oct. 29, 2019) (citation omitted).

⁸ Petitioner incorrectly asserts that collateral estoppel applies to its alleged motivation to combine *Jungck*'s embodiments. See Pet. at 31. The previously challenged claims did not include the "entire interface" or "all traffic" limitations. See §§ VI.A.1 and VI.A.2, *supra*. Prior Board proceedings involving materially different claim limitations "do not relieve Petitioner of its burden to identify the specific challenge." *Costco Wholesale Corp. v. Robert Bosch LLC*, IPR2016-00042, Paper 28 at 3–5 (P.T.A.B. July 7, 2016).

Here, Petitioner fills its claim chart with summaries of cherry-picked features from *Jungck*'s different embodiments and excerpts from different paragraphs of *Jungck*. See Pet. at 37–65. But “[i]t is not sufficient to demonstrate that each of the components in a challenged claim is known in the prior art; Petitioner must also explain why a person having ordinary skill in the art would have combined the elements disclosed in the separate embodiments described” in *Jungck*. *Samsung SDI Co. v. UBE Indus., Inc.*, IPR2017-02116, Paper 8 at 21–23 (P.T.A.B. Mar. 12, 2018) (citing *KSR*, 550 U.S. at 418); *In re Stepan Co.*, 868 F.3d 1342, 1346–48 (Fed. Cir. 2017); *Abiomed, Inc. v. Maquet Cardiovascular, LLC*, IPR2017-01204, Paper 8 at 8–12 (P.T.A.B. Oct. 23, 2017).

Petitioner's treatment of *Jungck* in the claim chart for elements [1.pre]–[1.a] that include the “entire interface” and “all traffic” limitation exemplifies its failure to explain how and why a skilled artisan would have combined *Jungck*'s different embodiments in the claimed manner. Pet. at 37–39, 42–43. Not only does Petitioner ignore *Jungck*'s edge caches and DNS translations (§ VI.A.1, *supra*) but Petitioner does not meaningfully explain why a skilled artisan would have been motivated to combine the any specific feature from *Jungck*'s different embodiments to result in edge servers that “collectively provide an entire interface” across *Jungck*'s POPs (the alleged boundary) or “packet filtering rules [being] applied to all network traffic traversing” those POPs. *Id.* at 37–38, 41–42

([1.pre]–[1.a]).

First, for both limitations, Petitioner begins by referring to its generic motivations to combine *Jungck*'s third through fifth embodiments, which are not tied to any claim language. *Id.* at 38, 42–44; § VI.A.3.1, *supra*. The fact that Petitioner's asserted motivations regurgitate those in the 1443, 1444, and 1513 IPRs without addressing the new “entire interface” and “all traffic” limitations shows that Petitioner's motivations bear no relationship to challenged claims. *Compare* Pet. at 31–33 with Ex. 1014 at 29–32, Ex. 1016 at 29–32, and Ex. 1012 at 12–19.

Second, Petitioner points to the prior Board decisions, arguing that “*Jungck* ‘broadly teach[es] protecting entire networks’ and [a skilled artisan] ‘would have found it obvious to apply the protective measures taught by *Jungck* to all the machines on a network because the artisan would have recognized that omitting restrictions based on subscriptions is simpler and advantageously protects the entire network.’” Pet. at 38–39 ([1.pre]) (quoting Ex. 1012 at 24). But Petitioner's argument is both conclusory and a non sequitur. Petitioner never explains why applying rules regardless of subscription status “to all the machines on a network” would have led to rules being “applied to all network traffic traversing” *Jungck*'s POPs. Petitioner fails to bridge the gap between applying rules to “all the machines on a network” (*id.* at 38) on the one hand and applying rules to “all

network traffic traversing [a] boundary” of a network as claimed.

Third, Petitioner provides additional motivations for its two alternative interpretations of the claims: assuming the claims require (1) “multiple PSGs” or (2) “multiple **POPs** each having at least one **edge server**”—which again are not claim limitations. *Id.* at 39 (emphasis added). Even so, “handl[ing] overload” or “failure” of a packet security gateway with redundancy (multiple edge servers) or protecting a LAN with multiple devices and entry points using multiple POPs each with one or more packet security gateways does not address the claim requirement that the packet security gateways “collectively provide an entire interface.” *See id.* As *Jungck* illustrates, the mere existence of multiple edge servers at a network boundary does not preclude network paths that bypass those edge servers. *See* § VI.A.1, *supra*.

Finally, when discussing the “ingress and egress filtering” performed by the “device 900” of *Jungck*’s fifth embodiment, Petitioner contends that a skilled artisan would have found it obvious to compare “all packets entering or leaving the protected network” to “blocklists (or another rule) to ‘ensur[e] that packets arriving from a particular network portion of the network actually came from that portion of the network’” and that “a POSITA would have been motivated to apply filtering rules to all such packets to prevent malicious intrusions.” *Id.* at 44 (quoting Ex. 1051, ¶ [0269]) (further citations omitted). This is a tacit admission that

Jungck does not disclose the “all traffic” limitation. See § VI.A.2, *supra*.

Moreover, “device 900” is not an edge server at a POP, but rather a single device connected to “network 100” (which is not a POP) that filters upstream and downstream packets it happens to receive (and not “all packets entering and leaving” *Jungck*’s network as a whole). Ex. 1051, ¶¶ [0266], [0268]. Petitioner does not explain why *Jungck*’s limited teaching of intercepting and processing upstream and downstream packets received by one device (“device 900”) establishes that *Jungck*’s “device 900” intercepts and processes “all packets entering and leaving” that network. Nor does Petitioner explain how and why that limited disclosure processing received packets at one device would be used to modify the edge server/edge cache arrangement at the POPs in *Jungck* so that all packets traversing the POP (the alleged boundary) are filtered according to the rules at all devices.⁹

⁹ Petitioner’s reliance on *Boston Scientific Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982 (Fed. Cir. 2009) (Pet. at 32) is misplaced. 554 F.3d at 990–91. There the Federal Circuit agreed the prior art patent’s two embodiments would be combined in the claimed manner based on specific findings that the first embodiment would have benefitted from a feature in the second embodiment. *Id.* Here, however,

Petitioner's asserted motivation and rationale of "applying filtering rules to all packets entering and leaving a network . . . to prevent malicious intrusions" (Pet. at 44) and constitutes improper hindsight reasoning as it appears to relate to features of *Jungck*'s third embodiment, which already "monitor[s] the data transmission . . . for malicious program code . . . or other unauthorized data being transmitted" and "performs ingress filtering." *Id.* (citing Ex. 1051, ¶¶ [0111], [0113]); see also *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1369 (Fed. Cir. 2012) (concluding hindsight provided the only reason to combine references describing devices that independently operated effectively to provide similar functions).

At bottom, Petitioner's claim chart improperly uses the challenged claims as a roadmap to reconstruct the claim elements in their recited arrangement. But "[i]t is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is obvious." *In re Suong-Hyu Hyon*, 679 F.3d 1363, 1371 (Fed. Cir. 2012) (quoting *In re Fritch*, 972 F.2d 1260, 1265 (Fed. Cir. 1992)); *SIBIA Neurosciences, Inc. v. Cadus Pharm. Corp.*, 225 F.3d 1349, 1360 (Fed. Cir. 2000).

Petitioner's motivations include no reference to the challenged claim limitations and, as explained above, are facially deficient. Pet. at 31–33, 37–65.

Petitioner's deficient explanation of why and how the different features it selects from across *Jungck*'s different embodiments would have rendered the independent claims obvious cannot support institution. *Johns Manville*, Paper 9 at 13–14; *Costco*, Paper 28 at 3.

B. Petitioner Has Not Demonstrated that the Art Discloses an SPMS Automatically Creating or Altering Rules

Petitioner provides no basis to support its assertion that *Jungck*'s external devices “create and modify [the] rules automatically.” Pet. at 47–48 ([1.c]). While *Jungck*'s rules “may be redefined or reset dynamically,” Petitioner cites no teaching in *Jungck* that such dynamic resetting or redefining is “automatic.” Ex. 1051, ¶ [0157] (resetting and redefining rules only “as needed”). *Jungck* describes other aspects of its embodiments that are “automatic,” but none includes resetting or redefining rules. *Id.*, ¶¶ [0039] (pushing email), [0059]–[0060] (translation requests), [0065] (switching IP addresses), [0130] (forwarding packets), [0155]–[0156] (capturing and releasing packets), [0202] (forwarding traffic statistics).

Petitioner's assertion that it would have been “obvious to automatically create/modify [*Jungck*'s] rules” is also lacking. Pet. at 48. First, Petitioner's

reliance on the 1443 FWD and 1386 FWD¹⁰ is misplaced because there the Board did not address whether it would have been obvious to automatically create or modify rules. *Id.* (citing Ex. 1014 at 46–48, Ex. 1018 at 21–22). In neither case did the challenged claims recite that rules were “automatically created or altered.” Ex. 1006 at 22:19–27; Ex. 1007 at 25:15–23. Instead, the Board addressed a claimed requirement of simply generating rules (1443 FWD) and explained how “dynamic security policy” should be understood in the context of the challenged claims (1386 FWD). Ex. 1014 at 46–48; Ex. 1018 at 20–22. And “dynamic” is not the same as “automatic.” *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1119–20 (Fed. Cir. 2004) (different words in a patent have different meanings). “[D]ynamic security policy” has never been understood as involving automation, but merely that the policy can be changed. Pet. at 20, n.9 (noting previous constructions of “dynamic security policy”); Ex. 1001 at 9:14–20, 13:41–50, 14:9–39. The ’266 Patent explains, an SPMS can “**automatically** create or alter” rules of such policies. *Id.* at 14:17–20 (emphasis added). Second, Petitioner’s reliance on MPEP § 2144.04 (Pet. at 48) is misguided as Petitioner overlooks the fact that the Examiner already considered and dismissed the notion

¹⁰ Invalidating claims of U.S. Patent No. 9,565,213 (Ex. 1018).

that automatically creating or altering rules would have been obvious. Ex. 1002 at 334–36 (allowance emphasizing “automatically created or altered” language).

Wood does not cure this deficiency. The cited portions of *Wood* describe updating lists of suspect addresses, not rules. Pet. at 49, 51–53 (citing Ex. 1052, ¶¶ [0034] (“suspect addresses 206 are updated as any one of the suspect address sources 210 receives a change to its suspect address data”), [0036] (“[w]ith each suspect address update (or some frequency), the adaptive interrogation module 304 reconfigures the router 306 with a new set of suspect addresses, if any changes to the suspect address list have been made”)). Although Petitioner cites *Wood*'s disclosures of configuring or reconfiguring *Wood*'s router, Petitioner does not show that this involves automatically creating or altering rules. *Id.* at 30, 52 (citing Ex. 1052, ¶¶ [0021], [0032], [0034]). Petitioner fails to show that *Jungck*, whether or not combined with *Wood* teaches “automatically created or altered” “packet filtering rules” as claimed ([1.c], [8.e], [15.c], [21.a]). *Id.* at 47–54.

C. Petitioner Has Not Shown that *Jungck*'s External Devices Update Rules Based on “Updated Malicious Traffic Information” Received from a “Malicious Host Tracker Service”

To show the claimed “updated malicious traffic information” ([1.e]), Petitioner relies only on updated lists of network addresses as described in *Jungck* and *Wood* such as IP addresses to block, sources of malicious program code, or other suspect addresses. Pet. at 33, 35, 56–57 (no allegation collateral estoppel

applies). Petitioner also relies on *Jungck*'s teachings that its external devices can redefine or reset rules and rulesets. *Id.* at 56 (citing Ex. 1051, ¶¶ [0157], [0160], [0175]). But regardless of whether updated lists of network addresses are received from *Jungck*'s virus watch service or Wood's sources, Petitioner does not sufficiently explain why or how *Jungck*'s external devices (the alleged SPMS) would have updated any rules based on the updated network addresses received.

Petitioner appears to overlook that *Jungck*'s packet interceptor adapter maintains the rules separate from network address blocklists, storing rules in non-volatile memory (812) and the blocked IP addresses in content addressable memory (816). Ex. 1051, ¶¶ [0130] (describing adaptor 720 of *Jungck*'s fourth embodiment), [0159] (more detailed description of adapter 720/800), [0165], [0176]–[0177], FIGS. 7–8. *Jungck* explains that the adapter stores blocked IP addresses in content addressable memory to benefit from efficiencies achieved with such memory when performing table lookups or matching values to table entries. *Id.*, ¶¶ [0165], [0176]–[0177], [0300].

Petitioner does not sufficiently explain why *Jungck*'s external devices—even if receiving updated lists of network addresses—would have had any reason to update *Jungck*'s rules rather than the separately stored, blocked IP addresses. *See id.*, ¶ [0300] (describing efficiencies associated with using content addressable memory); Ex. 1052, ¶ [0036] (“[w]ith each suspect address update (or some

frequency), the adaptive interrogation module 304 reconfigures the router 306 with a **new set of suspect addresses**)” (emphasis added). Indeed, *Jungck* describes a blanket rule that “checks the source IP address of [a] packet against a list of blocked IP addresses” and deletes the packet “[i]f the source IP address matches a blocked IP address stored in the content addressable memory.” Ex. 1051, ¶¶ [0176]–[0177].

Petitioner does not explain how a rule such as this, or any other rule, would change upon receiving a list of updated network addresses. Instead, Petitioner simply asserts without further explanation or analysis that a skilled artisan “would have understood that a rule set is first used to filter packets . . . then the rule set is ‘reset dynamically’ in any of the external devices.” Pet. at 56 (citing Ex. 1004, ¶ 288). Petitioner provides no details on what it means to dynamically reset rules used to filter packets or how such rules, once reset, would have been modified or redefined based on the list of updated network addresses received. *Id.*

While Petitioner’s expert alleges that *Jungck*’s rules would have been “‘reset dynamically’ . . . to **integrate** new malicious information (*e.g.*, new malicious code and/or suspect IP addresses) as they are discovered” (Ex. 1004, ¶ 288 (emphasis added)), the petition does not mention this concept of “integrat[ing] new malicious information” into *Jungck*’s rules. Petitioner cannot rely on this without improper incorporation by reference and further violation of the word limits. But, even then,

Petitioner's expert likewise appears to overlook the physical separation of *Jungck's* rules and block lists.

Petitioner thus fails to show that *Jungck's* external devices, whether or not combined with Wood's teachings, would have provided an "updated second set of packet filtering rules . . . that[] comprise an update to the . . . first packet filtering rules . . . based on updated malicious traffic information received from the at least one third party malicious host tracker service" as claimed ([1.e], [8.g], [15.e], [21.c]). Pet. at 55–58.

VII. CONCLUSION

Petitioner has not established a reasonable likelihood that it will prevail in establishing that Challenged Claims 1–27 of the '266 Patent are invalid. Patent Owner accordingly requests that the Board deny institution of *inter partes* review of the '266 Patent.

Patent Owner's Preliminary Response
IPR2021-01154 (U.S. Patent No. 10,785,266)

Respectfully submitted,

Dated: October 25, 2021

/James Hannah/

James Hannah (Reg. No. 56,369)
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, CA 94025
Tel: 650.752.1700 Fax: 650.752.1800

Jeffrey H. Price (Reg. No. 69,141)
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: 212.715.7502 Fax: 212.715.8302

Scott M. Kelly (Reg. No. 65,121)
Blair A. Silver (Reg. No. 68,003)
Bradley C. Wright (Reg. No. 38,061)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Tel: (202) 824-3000 Fax: (202) 824-3001

(Case No. IPR2021-01154)

Attorneys for Patent Owner

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

The undersigned hereby certifies that the portions of the above-captioned
PATENT OWNER'S PRELIMINARY RESPONSE specified in 37 C.F.R.
§ 42.24 has 13,905 words in compliance with the 14,000 word limit set forth in
C.F.R. § 42.24(b)(1). This word count was prepared using the Microsoft Word
word-processing system used to prepare this paper.

Dated: October 25, 2021

By: /James Hannah/
James Hannah (Reg. No. 56,369)
Jeffrey H. Price (Reg. No. 69,141)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Tel: (650) 752-1700
Email: jhannah@kramerlevin.com
Email: jprice@kramerlevin.com

Scott M. Kelly (Reg. No. 65,121)
Blair A. Silver (Reg. No. 68,003)
Bradley C. Wright (Reg. No. 38,061)
BANNER & WITCOFF, LTD.
1100 13th Street, NW, Suite 1200
Washington, DC 20005
Tel: (202) 824-3000
Email: skelly@bannerwitcoff.com
Email: bsilver@bannerwitcoff.com
Email: bwright@bannerwitcoff.com

*Attorneys for Patent Owner
Centripetal Networks, Inc.*

CERTIFICATE OF SERVICE

The undersigned certifies that on October 25, 2021, a copy of **PATENT OWNER'S PRELIMINARY RESPONSE** was served on the Petitioner by emailing a copy to the following:

Scott A. McKeown
ROPES & GRAY LLP
2099 Pennsylvania Avenue, NW
Washington, D.C. 20006-6807
Phone: 202-508-4740
Fax: 617-235-9492
scott.mckeown@ropesgray.com

Mark D. Rowland
James Batchelder (*pro hac vice*)
Andrew Radsch (*pro hac vice*)
ROPES & GRAY LLP
1900 University Ave., 6th Floor
East Palo Alto, CA 94303-2284
Phone: 650-617-4000
Fax: 617-235-9492
mark.rowland@ropesgray.com
james.batchelder@ropesgray.com
andrew.radsch@ropesgray.com

By: /James Hannah/
James Hannah (Reg. No. 56,369)

*Attorney for Patent Owner
Centripetal Networks, Inc.*