

EX 1024

1 Thomas N. Millikan, Bar No. 234430  
TMillikan@perkinscoie.com  
2 Joseph P. Reid, Bar No. 211082  
JReid@perkinscoie.com  
3 Kyle R. Canavera, Bar No. 314664  
KCanavera@perkinscoie.com  
4 Ashlee E. Sherman, Bar No. 348085  
ASherman@perkinscoie.com  
5 Sarah M. Anderson, Bar No. 359690  
SAnderson@perkinscoie.com  
6 PERKINS COIE LLP  
11452 El Camino Real, Ste 300  
7 San Diego, California 92130-2080  
Telephone: +1.858.720.5700  
8 Facsimile: +1.858.720.5799

9 Andrew N. Klein, Bar No. 300221  
AKlein@perkinscoie.com  
10 Hessam Gharaviram, Bar No. 345690  
HGharaviram@perkinscoie.com  
11 PERKINS COIE LLP  
3150 Porter Drive  
12 Palo Alto, California 94304-1212  
Telephone: +1.650.838.4300  
13 Facsimile: +1.650.838.4350

14 Attorneys for Plaintiff NETSKOPE, INC.

15 **UNITED STATES DISTRICT COURT**  
16 **NORTHERN DISTRICT OF CALIFORNIA**  
17 **OAKLAND DIVISION**

18  
19 NETSKOPE, INC.,

20 Plaintiff,

21 v.

22 FORTINET, INC.,

23 Defendant.

Case No. 4:25-cv-02360-HSG

**PLAINTIFF NETSKOPE, INC.'S  
AMENDED OPENING CLAIM  
CONSTRUCTION BRIEF**

**TABLE OF CONTENTS**

|      |                                                                                              |    |
|------|----------------------------------------------------------------------------------------------|----|
| I.   | INTRODUCTION .....                                                                           | 1  |
| II.  | LEGAL STANDARD.....                                                                          | 1  |
| A.   | CLAIM CONSTRUCTION.....                                                                      | 1  |
| B.   | Indefiniteness .....                                                                         | 3  |
| III. | LEVEL OF SKILL IN THE ART.....                                                               | 3  |
| IV.  | ARGUMENT .....                                                                               | 4  |
| A.   | '336 Patent .....                                                                            | 4  |
| 1.   | “shared network” ('336 Patent, claims 1-2, 4, 6-9, 11, 13-17, 20) .....                      | 4  |
| B.   | '710 Patent .....                                                                            | 5  |
| 1.   | “a network access gateway device” ('710 Patent, claim 15) .....                              | 5  |
| 2.   | “subordinate to” ('710 Patent, claims 1, 6, 8, 13, 15, 20).....                              | 8  |
| C.   | '426 Patent .....                                                                            | 10 |
| 1.   | “proxy for access sessions to the other services” ('426 Patent, claim 1) .....               | 10 |
| 2.   | “Principal believing interactions are with the external service” ('426 Patent, claim 1)..... | 12 |
| D.   | '936 Patent .....                                                                            | 15 |
| 1.   | “snapshots” ('936 Patent, claims 1, 7-8, 12, 21-22).....                                     | 15 |
| 2.   | “anomaly” ('936 Patent, claims 1, 2, 10, 12, 13, 18).....                                    | 18 |
| E.   | '153 Patent .....                                                                            | 19 |
| 1.   | “arbitrary number of attributes” ('153 patent, claims 1, 10, and 15).....                    | 19 |
| F.   | '697 Patent .....                                                                            | 21 |
| 1.   | “generating an alert” ('697 Patent, claims 1, 15, 24).....                                   | 21 |
| 2.   | “service provider network” ('697 Patent, claims 1, 15, 24).....                              | 23 |

## TABLE OF AUTHORITIES

### CASES

|                                                                                                                               |      |
|-------------------------------------------------------------------------------------------------------------------------------|------|
| <i>Am. Med. Sys., Inc. v. Biolitec, Inc.</i> ,<br>618 F.3d 1354 (Fed. Cir. 2010).....                                         | 6, 8 |
| <i>AstraZeneca AB, Aktiebolaget Hassle, KBI-E, Inc. v. Mutual Pharmaceutical Co.</i> ,<br>384 F.3d 1333 (Fed. Cir. 2004)..... | 19   |
| <i>Biosig Instruments, Inc. v. Nautilus, Inc.</i> ,<br>783 F.3d 1374 (Fed. Cir. 2015).....                                    | 3    |
| <i>C.R. Bard, Inc. v. U.S. Surgical Corp.</i> ,<br>388 F.3d 858 (Fed. Cir. 2004).....                                         | 19   |
| <i>Catalina Mktg. Int’l, Inc. v. Coolsavings.com, Inc.</i> ,<br>289 F.3d 801 (Fed. Cir. 2002).....                            | 6, 7 |
| <i>Chef Am., Inc. v. Lamb Weston, Inc.</i> ,<br>358 F.3d 1371 (Fed. Cir. 2004).....                                           | 4    |
| <i>Curtiss-Wright Flow Control Corp. v. Velan, Inc.</i> ,<br>438 F.3d 1374 (Fed. Cir. 2006).....                              | 16   |
| <i>Decisioning.com, Inc. v. Federated Dep’t Stores, Inc.</i> ,<br>527 F.3d 1300 (Fed. Cir. 2008).....                         | 22   |
| <i>Dow Chem. Co. v. United States</i> ,<br>226 F.3d 1334, 56 USPQ2d 1014 (Fed.Cir.2000) .....                                 | 17   |
| <i>Eaton Corp. v. Rockwell Int’l. Corp.</i> ,<br>323 F.3d 1332 (Fed. Cir. 2003).....                                          | 7    |
| <i>ePlus, Inc. v. Lawson Software, Inc.</i> ,<br>700 F.3d 509 (Fed. Cir. 2012).....                                           | 3    |
| <i>Frans Nooren Afdichtingssystemen B.V. v. Stopaq Amcorr Inc.</i> ,<br>744 F.3d 715 (Fed. Cir. 2014).....                    | 3    |
| <i>GE Lighting Sols., LLC v. AgiLight, Inc.</i> ,<br>750 F.3d 1304 (Fed. Cir. 2014).....                                      | 2    |
| <i>Georgetown Rail Equip. Co. v. Holland, L.P.</i> ,<br>867 F.3d 1229 (Fed Cir. 2017).....                                    | 7    |
| <i>Howmedica Osteonics Corp. v. Zimmer, Inc.</i> ,<br>640 Fed. Appx. 951 (Fed. Cir. 2016) .....                               | 6    |

|    |                                                          |        |
|----|----------------------------------------------------------|--------|
| 1  | <i>InterDigital Commc'ns, LLC v. Int'l Trade Comm'n,</i> |        |
| 2  | 690 F.3d 1318 (Fed. Cir. 2012).....                      | 16     |
| 3  | <i>Johnson Worldwide Assocs., Inc. v. Zebco Corp.,</i>   |        |
| 4  | 175 F.3d 985 (Fed. Cir. 1999).....                       | 22     |
| 5  | <i>Luminara Worldwide, LLC v. Liown Elecs. Co.,</i>      |        |
| 6  | 814 F.3d 1343 (Fed. Cir. 2016).....                      | 2      |
| 7  | <i>Mantech Env't Corp. v. Hudson Env't Servs., Inc.,</i> |        |
| 8  | 152 F.3d 1368 (Fed. Cir. 1998).....                      | 8      |
| 9  | <i>Microsoft Corp. v. i4i Ltd. P'ship,</i>               |        |
| 10 | 131 S.Ct. 2238 (2011).....                               | 14     |
| 11 | <i>Nautilus, Inc. v. Biosig Instruments, Inc.,</i>       |        |
| 12 | 572 U.S. 898 (2014).....                                 | 3      |
| 13 | <i>Omega Eng'g, Inc. v. Raytek Corp.,</i>                |        |
| 14 | 334 F.3d 1314 (Fed. Cir. 2003).....                      | 1      |
| 15 | <i>Phillips v. AWH Corp.,</i>                            |        |
| 16 | 415 F.3d 1303 (Fed. Cir. 2005).....                      | passim |
| 17 | <i>Rexnord Corp. v. Laitram Corp.,</i>                   |        |
| 18 | 274 F.3d 1336 (Fed. Cir. 2001).....                      | 2      |
| 19 | <i>Schumer v. Lab'y Comput. Sys., Inc.,</i>              |        |
| 20 | 308 F.3d 1304 (Fed. Cir. 2002).....                      | 7      |
| 21 | <i>STX, LLC v. Brine, Inc.,</i>                          |        |
| 22 | 211 F.3d 588 (Fed. Cir. 2000).....                       | 7      |
| 23 | <i>Teleflex, Inc. v. Ficosa N. Am. Corp.,</i>            |        |
| 24 | 299 F.3d 1313 (Fed. Cir. 2002).....                      | 10     |
| 25 | <i>Thorner v. Sony Comput. Ent. Am. LLC,</i>             |        |
| 26 | 669 F.3d 1362 (Fed. Cir. 2012).....                      | 2, 11  |
| 27 | <i>Vitronics Corp. v. Conceptiontronic, Inc.,</i>        |        |
| 28 | 90 F.3d 1576 (Fed. Cir. 1996).....                       | 2      |
|    | <b>STATUTES</b>                                          |        |
|    | 35 U.S.C. § 112, ¶ 2 .....                               | 3      |

## 1 I. INTRODUCTION

2 The Court should grant Plaintiff Netskope, Inc.’s (hereinafter “Netskope” or “Plaintiff”)  
 3 proposed constructions—plain and ordinary meaning—for each of the disputed claim terms  
 4 because they are guided by the intrinsic record. This approach not only respects the claim language  
 5 but also aligns with the specification and prosecution history. Indeed, Netskope’s plain and ordinary  
 6 meaning constructions are appropriate because (i) the claim terms would be readily understood by  
 7 a person of ordinary skill in the art (“POSITA”), and (ii) Netskope does not import language that  
 8 the patentees neither drafted nor disclaimed.

9 The proposed claim constructions of Defendant Fortinet, Inc. (hereinafter “Fortinet” or  
 10 “Defendant”) reflect Fortinet’s fundamental misunderstanding of the Court’s role in the claim  
 11 construction process. Fortinet views this process not as an opportunity to resolve disputes about the  
 12 scope of the asserted claims, but rather as (1) a chance to manufacture noninfringement positions,  
 13 and (2) an opportunity to attempt to invalidate claims through false ambiguity—despite the fact  
 14 that those terms would have been readily understood by a POSITA based on their written  
 15 description. Neither of these approaches are correct, and the Court should not indulge Fortinet’s  
 16 flawed claim construction positions. The Court should also reject Fortinet’s indefiniteness  
 17 arguments because Fortinet has failed to meet its burden to show that any term clearly and  
 18 convincingly fails to provide reasonable certainty as to its scope. Instead, the Court should leave  
 19 the claim terms as they are, using the language the patentee chose for the claimed subject matter.

## 20 II. LEGAL STANDARD

### 21 A. CLAIM CONSTRUCTION

22 Claim terms are generally given their customary meaning as understood by a POSITA at  
 23 the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 13113 (Fed. Cir. 2005). In fact,  
 24 there is a “‘heavy presumption’ that claim terms carry their full ordinary and customary meaning,  
 25 unless the patentee unequivocally imparted a novel meaning to those terms or expressly  
 26 relinquished claim scope during prosecution.” *Omega Eng’g, Inc. v. Raytek Corp.*, 334 F.3d 1314,  
 27 1323 (Fed. Cir. 2003) (internal citation omitted); *also* “[t]he words of a claim are generally given  
 28

1 their ordinary and customary meaning as understood by a person of ordinary skill in the art ...  
 2 [t]here are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts  
 3 as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in  
 4 the specification or during prosecution.” *Thorner v. Sony Comput. Ent. Am. LLC*, 669 F.3d 1362,  
 5 1365 (Fed. Cir. 2012) (internal citation omitted).

6 The standards for finding lexicography and disavowal are “exacting.” *GE Lighting Sols.,*  
 7 *LLC v. AgiLight, Inc.*, 750 F.3d 1304, 1309 (Fed. Cir. 2014). To act as a lexicographer, a patentee  
 8 must “clearly set forth a definition of the disputed claim term” and “clearly express an intent to  
 9 redefine the term.” *Thorner*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citation modified). While  
 10 disavowal requires that “the specification [or prosecution history] make[] clear that the invention  
 11 does not include a particular feature.” *Luminara Worldwide, LLC v. Liown Elecs. Co.*, 814 F.3d  
 12 1343, 1353 (Fed. Cir. 2016) (quoting *SciMed Life Sys. Inc. v. Advanced Cardiovascular Sys., Inc.*,  
 13 242 F.3d 1337, 1341 (Fed. Cir. 2001).). Such disavowal can occur either explicitly or implicitly,  
 14 but it must be clear and unmistakable. *Id.*

15 Where claim terms are disputed, intrinsic evidence must be considered first as it is “the most  
 16 significant source of the legally operative meaning of disputed claim language.” *Vitronics Corp. v.*  
 17 *Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). Specifically, the claim language  
 18 “provide[s] substantial guidance as to the meaning of particular claim terms.” *Phillips*, 415 F.3d at  
 19 1314. However, claims do “not stand alone”; rather, they “are part of a fully integrated written  
 20 instrument” and thus must be read in view of the specification. *Phillips*, 415 F.3d at 1315 (citation  
 21 modified). “If the term or terms chosen by the patentee so deprive the claim of clarity that there is  
 22 no means by which the scope of the claim may be ascertained by one of ordinary skill in the art  
 23 from the language used, a court must look to the specification and file history to define the  
 24 ambiguous term.” *Rexnord Corp. v. Laitram Corp.*, 274 F.3d 1336, 1343 (Fed. Cir. 2001) (citation  
 25 modified). Thus, after the language of the claims themselves, the Court should consider the rest of  
 26 the intrinsic evidence, beginning with the specification and finishing with the prosecution history.  
 27 *Id.*

Courts may also consider extrinsic evidence, such as technical dictionaries or expert testimony “that can assist the court in determining the meaning of particular terminology to those of skill in the art.” *Phillips*, 415 F.3d at 1318. “Terms generally carry their ordinary and customary meaning in the relevant field at the relevant time, as shown by reliable sources such as dictionaries, but they always must be understood in the context of the whole document—in particular, the specification (along with the prosecution history, if pertinent).” *Frans Nooren Afdichtingssystemen B.V. v. Stopaq Amcorr Inc.*, 744 F.3d 715, 722 (Fed. Cir. 2014).

### **B. Indefiniteness**

“[I]ndefiniteness is a question of law and in effect part of claim construction.” *ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 517 (Fed. Cir. 2012). Patent claims must particularly point out and distinctly claim the subject matter regarded as the invention. 35 U.S.C. § 112, ¶ 2. Whether a claim is indefinite is determined from the perspective of a POSITA as of the time the application was filed. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 908 (2014).

A patent claim is indefinite only if, when “read in light of the specification delineating the patent, and the prosecution history, [the claim] fail[s] to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). “Reasonable certainty” does not require “absolute or mathematical precision.” *Biosig Instruments, Inc. v. Nautilus, Inc.*, 783 F.3d 1374, 1381 (Fed. Cir. 2015). And, indefiniteness must be proven by clear and convincing evidence. *Id.* at 1377.

### **III. LEVEL OF SKILL IN THE ART**

As of the filing dates of the U.S. Patent Nos. 8,356,336 (the “‘336 Patent”), 8,543,710 (the “‘710 Patent”), 8,327,426 (the “‘426 Patent”), 7,593,936 (the “‘936 Patent”), 8,661,153 (the “‘153 Patent”), and 8,635,697 (the “‘697 Patent”), a POSITA would have a B.S. in computer science, computer engineering, or electrical engineering (or equivalent) and at least two years’ experience in computer networking and security.

1 **IV. ARGUMENT**

2 **A. '336 Patent**

3 **1. “shared network” ('336 Patent, claims 1-2, 4, 6-9, 11, 13-17, 20)**

| Netskope's Construction    | Fortinet's Construction                                       |
|----------------------------|---------------------------------------------------------------|
| Plain and ordinary meaning | “a local network to which an unauthenticated user has access” |

6 The term “shared network” is composed of two ordinary, jury-friendly English words whose  
 7 meanings are clear and well-understood, particularly by a POSITA. Nothing in the intrinsic record  
 8 suggests any special lexicography or an intent by the patentee to redefine the term, nor is there any  
 9 indication of disavowal of claim scope. Accordingly, the Court should adopt the plain and ordinary  
 10 meaning of “shared network” as understood in the context of the patent.

11 In contrast, Fortinet asks this Court to construe “shared network” by adopting an improperly  
 12 narrow construction that lacks any intrinsic or extrinsic support. Considering Fortinet's proposed  
 13 construction repeats the word “network,” Fortinet's position is that the modifier “shared” restricts  
 14 “network” to only local use and unauthenticated users—limitations found nowhere in the patent.  
 15 The Federal Circuit has made clear that ordinary, simple English words generally do not require  
 16 construction, *see Chef Am., Inc. v. Lamb Weston, Inc.*, 358 F.3d 1371, 1373 (Fed. Cir. 2004)  
 17 (“[O]rdinary, simple English words whose meaning is clear and unquestionable . . . mean exactly  
 18 what they say.”), and the Court should reject Fortinet's attempt to impose unsupported restrictions.

19 The term “network” has long been understood in the technical field to mean a group of  
 20 computers or devices connected by communication facilities. Ex. 1 at 362. This definition has been  
 21 recognized for decades and applies broadly to networks of any size—from small networks with  
 22 only a few devices to networks spanning a large geographic area, such as wide area networks  
 23 (WANs). Nothing in this definition imposes a requirement that the network be local, versus wide  
 24 area, versus other geographical arrangements. And, nothing in this definition imposes a requirement  
 25 that the network be limited to any particular type or class of user, such as “unauthenticated users.”  
 26 By requiring the network to be “local” and limited to “unauthenticated users,” Fortinet proposes a  
 27 construction that includes two different supposed disclaimers, but without any support whatsoever  
 28 for either in the intrinsic record. Indeed the specification never once mentions a “local network,”

1 and it provides broad disclosure of the shared network, not limited by either of Fortinet’s proposed  
2 disclaimers. *See* ’336 Patent at 5:45-67.

3 Instead, courts look to “the claims of a patent define the invention to which the patentee is  
4 entitled.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (quoting *Innova/Pure*  
5 *Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). Here, not  
6 only is the claim language “shared network” easily understood, but the claims provide further  
7 information on what the shared network comprises: “providing a network access controller in a  
8 shared network, **wherein the shared network comprises** a plurality of server computers and a set  
9 of network destinations hosted on the plurality of server computers.” ’336 Patent at claim 1. This  
10 additional contextual description is consistent with the broad, well-understood meaning discussed  
11 above, and lacks support for either of Fortinet’s proposed disclaimers.

12 Without any textual support in the specification, Fortinet points to Figure 1 and 2 as the  
13 basis for its narrowed construction. Ex. 2 at 1. However, neither of those figures provide support  
14 for Fortinet’s two proposed restrictions. Even if they did show a local network and/or an  
15 unauthenticated user, the accompanying descriptions for both figures explicitly state that these are  
16 exemplary embodiments. ’336 Patent at 3:1-6 and 4:37-40. It would not be appropriate to restrict  
17 the claims to that single embodiment when the claims do not recite that feature. *Phillips*, 415 F.3d  
18 at 1323 (“To avoid importing limitations from the specification into the claims, it is important to  
19 keep in mind that the purposes of the specification are to teach and enable those of skill in the art  
20 to make and use the invention”).

21 Fortinet’s proposed construction improperly imports two separate claim scope disclaimers  
22 without any meaningful intrinsic or extrinsic support. For these reasons, the Court should adopt  
23 Netskope’s plain and ordinary meaning construction, which is fully supported by the claim  
24 language and understanding of a skilled artisan.

## 25 **B. ’710 Patent**

### 26 **1. “a network access gateway device” (’710 Patent, claim 15)**

| Netskope’s Construction    | Fortinet’s Construction |
|----------------------------|-------------------------|
| Plain and ordinary meaning | Preamble is limiting    |

1 The preamble of claim 15 to the '710 Patent is not limiting because it does not provide  
 2 essential structure to the limitations in the claim body. Under Federal Circuit precedent, a preamble  
 3 is limiting only in narrow circumstances where either the preamble is required to understand the  
 4 body of the claim, or the applicant clearly relied on it to distinguish the claimed invention from the  
 5 prior art. Here, the body of claim 15 is complete on its own, and nothing in the intrinsic record  
 6 elevates the preamble to be limiting. Accordingly, the Court should reject Fortinet's construction.

7 Courts generally presume that the preamble does not limit the claims. *Am. Med. Sys., Inc.*  
 8 *v. Biolitec, Inc.*, 618 F.3d 1354, 1358 (Fed. Cir. 2010) (quoting *Allen Eng'g Corp. v. Bartell Indus.*,  
 9 299 F.3d 1336, 1346 (Fed. Cir. 2002)). A preamble is limiting "if it recites essential structure or  
 10 steps, or if it is necessary to give life, meaning, and vitality to the claim." *Am. Med. Sys.* at 1358.  
 11 (citation modified). However, a preamble is not limiting "when the claim body describes a  
 12 structurally complete invention such that deletion of the preamble phrase does not affect the  
 13 structure or steps of the claimed invention." *Id.* at 1358-59. The Federal Circuit has provided some  
 14 "guideposts" to determine when the preamble may be limiting, such as: the preamble is essential to  
 15 understand limitations or terms in the claim body; the preamble recites "additional structure or steps  
 16 underscored as important by the specification," "clear reliance on the preamble during prosecution  
 17 to distinguish the claimed invention from the prior art," and the preamble provides antecedent basis.  
 18 *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002).

19 Claim 15's preamble is not limiting because the body of the claim recites a structurally  
 20 complete invention that does not need the preamble to breathe "life, meaning, and vitality" thereto.  
 21 In particular, the body of claim 15 recites at least one computer processor and at least one storage  
 22 medium with computer instructions that cause the processor to perform a plurality of quarantine  
 23 control functions and rendering of a web page. *See* '710 Patent at claim 15. Claim 15's preamble  
 24 is not essential to understand these requirements, and the deletion of the preamble would not affect  
 25 the disclosed structure. *Howmedica Osteonics Corp. v. Zimmer, Inc.*, 640 Fed. Appx. 951, 956 (Fed.  
 26 Cir. 2016) ("The body of each claim describes a structurally complete invention...and deletion of  
 27 the preamble language does not affect that structure"). Instead, the preamble merely gives a name  
 28

1 (“network access gateway device”) to a structurally complete invention that would operate the same  
2 regardless of whether that name is attached to it or not. *See* ’710 Patent at claim 15. *See also* *Eaton*  
3 *Corp. v. Rockwell Int’l. Corp.*, 323 F.3d 1332, 1339 (Fed. Cir. 2003) (“On the other hand, ‘[i]f the  
4 body of the claim sets out the complete invention,’ then the language of the preamble may be  
5 superfluous.”).

6 Moreover, “a network access gateway device” merely recites an apparatus for performing  
7 a plurality of quarantine control functions over a client device—all of which are separately recited  
8 in the body of the claim—which weighs against finding the preamble limiting. *See* *STX, LLC v.*  
9 *Brine, Inc.*, 211 F.3d 588, 591 (Fed. Cir. 2000). “The language of the body of the claim ‘sets out  
10 the complete invention’ in that it provides in detail the functional attributes of the device that  
11 performs the methods.” *Schumer v. Lab’y Comput. Sys., Inc.*, 308 F.3d 1304, 1310 (Fed. Cir.  
12 2002)(citation omitted). The preamble does not recite “additional structure or steps underscored as  
13 important by the specification.” *Catalina Mktg.*, 289 F.3d at 808-09. Indeed, the preamble of claim  
14 15 only discloses an apparatus—a network access gateway device. The preamble does not include  
15 any functions, features, or components of the apparatus that would provide any additional meaning  
16 to the claim. Further, a POSITA would readily understand which devices can manage network  
17 traffic for quarantine control. *See* ’710 Patent at 1:58-2:19.

18 Finally, during prosecution of the ’710 Patent, the applicant did not rely on claim 15’s  
19 preamble to distinguish the disclosed invention over the prior art—another factor favoring a finding  
20 that the preamble is not limiting. Fortinet relies on applicant’s arguments made on May 15, 2013  
21 to support its position. Ex. 2 at 2-3. However, neither the amendment, the accompanying remarks,  
22 nor any subsequent prosecution history reference the preamble of claim 15 or suggest that it  
23 imposes any limitation on the claim. *See* Ex. 3. Accordingly, the ’710 Patent’s prosecution history  
24 is silent as to any reliance on the preamble to distinguish over the prior art, thereby emphasizing its  
25 non-limiting nature. “Ambiguous statements made during prosecution, especially those that do not  
26 directly distinguish the element claimed as essential for purposes of finding a limitation in the  
27 preamble, cannot fairly limit the characteristics of the claim term.” *Georgetown Rail Equip. Co. v.*

*Holland, L.P.*, 867 F.3d 1229, 1238 (Fed Cir. 2017) (quoting *Grober v. Mako Prods., Inc.*, 686 F.3d 1335, 1342 (Fed. Cir. 2012) (citation modified)).

Accordingly, the preamble is not limiting because it does not give “life, meaning, and vitality” thereto. *Am. Med. Sys*, 618 F.3d at 1358.

## 2. “subordinate to” (’710 Patent, claims 1, 6, 8, 13, 15, 20)

| Netskope’s Construction    | Fortinet’s Construction |
|----------------------------|-------------------------|
| Plain and ordinary meaning | Indefinite              |

“Subordinate to” is a term that Fortinet asks the Court to construe as indefinite, even though the claims and specification provides sufficient clarity as to its meaning. Instead of looking to the ’710 Patent’s specification to interpret this term, Fortinet advances an indefiniteness theory but offers no evidence of any contradictory meaning. Fortinet provides no expert testimony or competing dictionary definitions. Fortinet’s indefiniteness argument rests solely on its say-so, and for these reasons, the Court should adopt Netskope’s plain and ordinary meaning construction.

“Under proper claim construction methodology, we look first to the language of the claims.” *Mantech Env’t Corp. v. Hudson Env’t Servs., Inc.*, 152 F.3d 1368, 1373 (Fed. Cir. 1998). The term “subordinate to” appears in claim 1 as follows:

1. A method of network traffic quarantine control, comprising:
  - at a network access gateway device between a local network and the Internet, selecting a client device in a first network segment of the network;
  - at the network access gateway device, performing a plurality of quarantine control functions over the client device, wherein the plurality of quarantine control functions comprises:
    - a) restricting all network traffic emanating from the client device to one or more network destination addresses that are not in or **subordinate to** the first network segment; ...

’710 Patent at claim 1 (emphasis added). The term “subordinate to” also appears in the same phrase in claims 6, 8, 13, 15, and 20. In the context of the specification and figures, nothing about this term would be difficult to understand by a POSITA. The specification describes the need for controlled environments, or “walled gardens,” which “limit the network segments or routes available...where a network client may be constrained in terms of the types of network protocols (and applications) that they are permitted network access, as well as the destinations or services to which network applications may connect.” ’710 Patent at 3:48-55. The specification further describes how using

1 walled gardens is valuable because it can “inform a user of certain conditions and still allow a user  
 2 access to a set of network destinations that may be helpful (for example, in resolving the condition  
 3 that led to reduced access).” *Id.* at 4:6-12. Essentially, the patent explains the need for a network  
 4 location that operates in some way independently of the broader network architecture, including  
 5 for additional purposes like preserving network security or implementing a paywall or authorization  
 6 requirement before a user may access network resources. Accordingly, the ability to have a network  
 7 location that is not “subordinate to” another network segment facilitates the achievement of these  
 8 objectives.

9 Indeed, this clear understanding is further reinforced by the ’710 Patent’s figures. For  
 10 example, Figure 1 depicts a network topology in which Clients 1, 2, 3, 4 connect to gateway 11,  
 11 which connects to the Internet. *See* Fig. 1. The Internet in Figure 1 comprises walled garden “A,”  
 12 which holds sites “K” and “M,” and walled garden “B,” which holds site “P” and shares site “M”  
 13 with walled garden “A.” *Id.* The Internet in Figure 1 also hosts walled garden “C,” which holds site  
 14 “S,” in which neither the walled garden “C” or site “S” is attached. *Id.* The specification further  
 15 describes an example configuration using the walled garden that is not subordinate to other network  
 16 resources:

17 “In one embodiment, the gateway may detect this infection based on  
 18 observed, detected behavior fitting a pattern that is suitable for  
 19 constraint. By assigning the client to a walled garden reserved for  
 infected users traffic from this client to destinations outside the  
 walled garden becomes restricted.”

20 ’710 Patent at 5:59-64. “The gateway’s web server renders a web page informing the client of its  
 21 perceived infection and offering links to self-help documents and to the websites of anti-virus  
 22 vendors and the client’s OS vendor. Thus, traffic from the client to the destination in the walled  
 23 garden for infected users is allowed while other traffic is denied or redirected.” *Id.* at 6:1-6. Once  
 24 again, the specification provides a specific, detailed example illustrating why it is necessary for a  
 25 network location to be separated from other network locations.

26 Finally, as Dr. Striegel explained in his expert declaration, a POSITA would have at least a  
 27 college degree in electrical engineering, telecommunications, computer engineering, computer

science, or a related technical field, along with two-three years of experience in related fields. Ex. 4 at ¶25. With that context, a POSITA would understand that “a network segment may be considered subordinate if it operates within the administrative, routing, or policy domain of another segment—regardless of physical or topological configuration.” *Id.* at ¶44.

The Federal Circuit established that “[i]n the absence of an express intent to impart a novel meaning to the claim terms, an inventor’s claim terms take on their ordinary meaning.” *Teleflex, Inc. v. Ficoso N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). “We indulge a ‘heavy presumption’ that a claim term carries its ordinary and customary meaning.” *Id.* Accordingly, in light of the extensive support in the specification, figures, claims, and Dr. Striegel’s testimony, the Court should adopt Netskope’s plain and ordinary meaning construction of “subordinate to.”

### C. ’426 Patent

#### 1. “proxy for access sessions to the other services” (’426 Patent, claim 1)

| Netskope’s Construction    | Fortinet’s Construction                              |
|----------------------------|------------------------------------------------------|
| Plain and ordinary meaning | “proxy for all communications to the other services” |

The meaning of this claim phrase is readily understood by a POSITA and does not require further construction. Indeed, Fortinet’s proposed construction seems to largely concede that point, because it leaves much of the claim language unchanged. Instead, Fortinet swaps out “access sessions” for the entirely distinct and much broader “all communications,” in an unnecessary, unsupported, and incorrect redefinition of that sub-phrase. There is no need to provide further construction of this phrase, much less to adopt Fortinet’s crude attempt to manufacture a non-infringement position out of whole cloth. The Court should adopt Netskope’s construction.

The ’426 Patent’s specification provides support for the plain language of this claim phrase, and no basis to redefine the sub-phrase “access sessions” as Fortinet proposes. The specification describes an “identity service” as a “special type of service that is designed to manage and supply authentication services and authentication information for principals and for other services.” ’426 Patent at 2:33-36. “So, an identity service may authenticate a given principal for access to a variety of local and external services being managed by that identity service. A single principal may have multiple identity services.” *Id.* at 2:36-39. Other passages in the specification also explain that “the

1 processing of the single sign-on services facilitates principal access to a variety of additional  
 2 identity services and other services accessible to the single sign-on service in an automated fashion  
 3 that may be transparent and seamless from the perspective of the principal.” *Id.* at 4:25-29. Based  
 4 on these descriptions, it is clear that the identity service serves as a proxy for “access sessions”  
 5 (e.g., authentication services) to the “other services” (e.g., local and external services managed by  
 6 that identity service) on behalf of the principal. However, the patent does not describe that this  
 7 proxy serves as the pathway for ***all communications*** to external services. Indeed, the specification  
 8 only describes that proxy serves as the communication between the authentication services and the  
 9 identity service the principal seeks access to.

10 Fortinet’s proposed construction is flawed because it would require the proxy to handle all  
 11 communications—for example, every single packet—once the session is established. The patent’s  
 12 written description does not require such an absolute requirement, leaving open the possibility that  
 13 some data packets may be communicated outside of the proxy. Claim terms “are generally given  
 14 their ordinary and customary meaning as understood by a POSITA when read in the context of the  
 15 specification and prosecution history.” *Thorner v. Sony Comput. Ent. Am. LLC*, 669 F.3d 1362,  
 16 1365 (Fed. Cir. 2012), (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005)). “There  
 17 are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his  
 18 own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the  
 19 specification or during prosecution.” *Thorner*, 669 F.3d at 1365.

20 Fortinet cites several portions of the ’426 specification, but none supports Fortinet’s  
 21 extreme attempt to rewrite this claim phrase. *See* Ex. 2 at 4. For example, Fortinet relies on the ’426  
 22 Patent specification at 3:17-21 and 3:54-61, but these passages do not provide anything like the sort  
 23 of redefinition of “access sessions” that Fortinet is seeking in its construction. Indeed, this text  
 24 merely reiterates the same plain language underscored by the term itself—that the proxy handles  
 25 the “single sign on,” which is relevant to an individual session. Contrary to Fortinet’s position,  
 26 these passages support Netskope’s plain & ordinary meaning construction—e.g., that the proxy  
 27 mediates ***session-level authentication*** and ***access control*** between a principal and the external  
 28

services. Moreover, none of Fortinet’s other citations to the specification support broadening this construction to include the proxy covering *all* to the external services. *See* Ex. 2 at 4. Instead, these portions of the patent merely reinforce the notion that the patent discloses a proxy for access sessions to the other services, but not necessarily all communications whatsoever.

Fortinet also cites two portions of the ’426 Patent’s file history as supposedly supporting its construction. But neither of these portions of the file history provide any better support. *See* Ex. 5. In Applicant’s November 24, 2009 Remarks, the applicant merely repeated the same scope recited by the plain language of the claim, i.e., that access sessions are proxied, not that all communications whatsoever to the external services are proxied. *Id.* at 1-12. In the March 25, 2010 Final Rejection, the Patent Examiner rejected claim 1 in view of two prior art references. *Id.* at 16-40. In the subsequent response, the applicant argued against that rejection by explaining why the prior art combination did not disclose a different limitation of claim 1. *Id.* at 48-60. Neither of Fortinet’s citations to the file history support its attempt to redefine “access sessions” to require the proxy to proxy “all communications” whatsoever.

Here, the patentee did not set out a definition requiring that the proxy handle all communications to the other services, nor did the patentee disavow the full scope of the claim—which would allow the proxying of access sessions, but not necessarily all communications whatsoever. Accordingly, Fortinet’s construction is improper and should be rejected.

**2. “Principal believing interactions are with the external service” (’426 Patent, claim 1)**

| Netskope’s Construction    | Fortinet’s Construction |
|----------------------------|-------------------------|
| Plain and ordinary meaning | Indefinite              |

“Principal believing interactions are with the external service” is another term that Fortinet asks the Court to construe as indefinite despite the claims and specification providing sufficient clarity as to the meaning. Fortinet provides no evidence as to why a POSITA would not understand this term. For the reasons explained below, the Court should adopt Netskope’s construction regarding this term.

“[T]he claims themselves provide substantial guidance as to the meaning of particular claim terms.” *Phillips*, 415 F.3d at 1314 (Fed. Cir. 2005). Fortinet provides no justification for why the

claim language itself fails to provide a reasonably certain meaning for this claim phrase. Claim 1 of the '426 Patent reads, in relevant part:

1. A machine-implemented method to execute on a machine, comprising:

...

supplying, by the machine, an authentication message for use by an identity service on behalf of the principal, the authentication message serves as a new authentication request and as a new authentication response for single sign-on access of the principal to the identity service and other services external or internal to the identity service, the identity service acts as a proxy for access sessions to the other services on behalf of the principal, the principal's access sessions occur indirectly through the identity service and transparently to the principal,

...

*the principal believing interactions are with the external service...*

Nothing about the claim term suggests that the phrase would lack understanding by a POSITA—indeed, even laymen and members of a jury would readily understand the scope of this term. The phrase is used to describe a principal's (e.g., an end user or end user's device) experience with the claimed invention, in which the principal believes it is interfacing directly with an external service and not an intermediary that connects the user to that external service. This is a "transparent proxy" architecture known in the art, Ex. 4 at ¶59, and described through examples in the specification:

"Initially, one or more identity services, such as enhanced versions of identity services disclosed and incorporated by reference above, include a variety of services that they perform authentication for to ensure legitimate access to those services. The identity services may control access to services that are local to them or that are external to them. Moreover, the identity services are trusted with one another and communicate securely with on[e] another."

'426 Patent at 3:54-61. The specification explains further that "[t]h presence of the single sign-on service may be *transparent or unknown to the principal*. That is, the principal may believe that it is interacting or attempting to interact with an external service and the single sign-on service intercepts the communication and attempts to authenticate the principal..." *Id.* at 4:9-15 (emphasis added). Thus, by executing transparently to the principal, the proxy operates such that the communications between the proxy and the external services are not perceived by the principal.

1 The specification provides additional examples of how the principal may believe its interactions  
2 are with the external service: “The combined new authentication request and new authentication  
3 response may be viewed as an authentication message supplied by the single sign-on service to the  
4 principal and perhaps *unbeknownst to the principal*.” *Id.* at 4:65-5:1 (emphasis added).

5 Despite the plain language of the claims and specification, Fortinet fails to identify how a  
6 POSITA would be unable to understand the language of the claim. Fortinet’s position for this term  
7 is further undermined when considering its *own* patent portfolio. Fortinet is listed as the assignee  
8 to multiple patents that refer to a “transparent proxy.” For example, Fortinet is the original assignee  
9 to U.S. Patent No. 9,825,988, “Content Filtering of Remote File-System Access Portfolios,” which  
10 provides “[m]ethods and systems for content filtering of remote file system access protocols...”  
11 ’988 Patent at Abstract. Fortinet’s ’988 Patent specification explains that “[t]he phrase ‘transparent  
12 proxy’ generally refers to a specialized form of proxy that only implements a subset of a given  
13 protocol and allows *unknown or uninteresting protocol commands to pass unaltered*.” *Id.* at 5:57-  
14 60. By stating that the transparent proxy performs “unknown or uninteresting” protocols to pass,  
15 Fortinet’s ’988 Patent describes processing that the principal is oblivious to, in which the principal  
16 must believe that it is interacting with the external service.

17 Fortinet fails to provide any evidence that a POSITA would find this term indefinite.  
18 Further, nowhere in the prosecution history does the U.S. Patent and Trademark Office indicate  
19 that this term is indefinite or that a POSITA would fail to understand the term in light of the  
20 specification. *See Microsoft Corp. v. i4i Ltd. P’ship*, 131 S.Ct. 2238, 2244 (2011) (affirming that a  
21 patent shall be presumed valid and that a challenger attacking the validity of patent claims has a  
22 statutory burden to prove invalidity by “clear and convincing” evidence).

23 Additionally, Fortinet fails to provide any expert testimony that a POSITA would not  
24 understand this term in light of the specification. Instead, Dr. Striegel explains how a POSITA  
25 would understand that a “principal believing interactions are with the external service” refers to the  
26 identity service acting as a transparent proxy between the principal and an external service, in which  
27 “the identity services handles requests and responses in a way that makes its mediation invisible.”

Ex. 4 at ¶59. “This enables a single sign-on framework across multiple services without the need for additional user logins or awareness of the proxying services occurring behind the scenes.” *Id.*

Accordingly, Fortinet has only attempted to manufacture ambiguity where none exists. Because the record provides ample support for the plain and ordinary meaning of “principal believing the interactions are with the external service,” the Court should adopt Netskope’s plain and ordinary meaning construction.

#### D. ’936 Patent

##### 1. “snapshots” (’936 Patent, claims 1, 7-8, 12, 21-22)

| Netskope’s Construction    | Fortinet’s Construction                                                                                                                                                                                                                          |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plain and ordinary meaning | “the state of a machine based on an examination of all system files, designated application files, the registry, performance counters, processes, services, communication ports, hardware configuration, and log files at a given point in time” |

The term “snapshots” should be construed according to its plain and ordinary meaning, as supported by the claim language and broad disclosure in the specification. Fortinet instead asks the Court to adopt a construction that requires a “snapshot” to include *nine* different component parts, amounting to what is effectively nine different claim term disclaimer positions. To support this extreme rewriting of the term, Fortinet cites an amalgamation of three unrelated technical dictionaries and cherry-picked citations from the specification, all of which disclose, perhaps, what a snapshot could contain. But none provide support for limiting a snapshot to even one of Fortinet’s component parts, much less all nine. The claims and specification consistently describe snapshots as data indicating the state of a computer, without imposing rigid requirements. The Court should reject Fortinet’s attempt to write nine different limitations into the meaning of “snapshot.”

As with other terms Fortinet seeks to complicate, examining the claim language itself provides the most clarity. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005). The claim itself tells us what a snapshot includes, and unsurprisingly given Fortinet’s many extreme positions, the claim describes none of the nine limitations that Fortinet attempts to import into the construction: “A method of detecting abnormal system states in computers, comprising: receiving

1 snapshots from a plurality of computers within a population of computers, ***wherein individual***  
 2 ***snapshots include data indicating a state of a respective computer...***’936 Patent at claim 1.  
 3 Fortinet ignores this straightforward language and attempts to read nine more specific limitations  
 4 into the meaning of “snapshot”—yet another crude attempt to manufacture a non-infringement  
 5 position where one does not exist.

6 Fortinet’s construction not only disregards the claim language but also violates the well-  
 7 established doctrine of claim differentiation by rendering dependent claims redundant. *InterDigital*  
 8 *Commc’ns, LLC v. Int’l Trade Comm’n*, 690 F.3d 1318, 1324 (Fed. Cir. 2012) (“[C]laim  
 9 differentiation is at its strongest in this type of case, ‘where the limitation that is sought to be ‘read  
 10 into’ an independent claim already appears in a dependent claim.’” (quoting *Liebel-Flarsheim Co.*  
 11 *v. Medrad, Inc.*, 358 F.3d 898, 910 (Fed. Cir. 2004))). Claim 7 reads: “The method of claim 1,  
 12 wherein individual snapshots include data associated with at least one of: system files, application  
 13 files, a registry entry, a performance counter, a process, a communication port, a hardware  
 14 configuration, a log file, a running task, services, and network connections.” ’936 Patent at claim  
 15 7. If Fortinet’s construction were adopted, claim 7—and similar dependent claims—would be  
 16 entirely superfluous, because claim 1 would already require the features that make up the entirety  
 17 of claim 7. Such redundancy is impermissible under established claim construction principles.  
 18 *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (holding that the presence of a  
 19 dependent claim adding a particular limitation gives rise to a presumption of claim differentiation  
 20 and that the limitation in question is not present in the independent claim).

21 Beyond garden variety violation of the claim differentiation doctrine, Fortinet’s proposed  
 22 construction violates that doctrine in new and creative ways. A typical, and improper, violation of  
 23 the claim differentiation doctrine would have incorporated the requirements of claim 7 into claim  
 24 1, and thereby rendered claim 7 redundant. “‘Claim differentiation’ refers to the presumption that  
 25 an independent claim should not be construed as requiring a limitation added by a dependent  
 26 claim.” *Curtiss-Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1380 (Fed. Cir. 2006)  
 27 (citation modified). If Fortinet had proposed such a construction, it would have been appropriate  
 28

1 for the Court to reject it. *Dow Chem. Co. v. United States*, 226 F.3d 1334, 1341–42, 56 USPQ2d  
2 1014, 1019–20 (Fed.Cir.2000) (applying the doctrine of claim differentiation and concluding that  
3 an independent claim should be given broader scope than a dependent claim to avoid rendering the  
4 dependent claim redundant). But Fortinet went much further here. Dependent claim 7 requires that  
5 the snapshot include ***at least one of*** the list of items. Fortinet’s proposed construction would require  
6 that a snapshot be created using ***all of*** the nine recited items. Fortinet has thus not simply  
7 incorporated a dependent claim into the independent claim and improperly violated the claim  
8 differentiation doctrine. Fortinet goes much further and proposes to make the independent claim  
9 nine-fold narrower than a claim that depends on it.

10 The specification confirms that “snapshot” has a flexible and broad meaning in the art and  
11 does not require Fortinet’s gratuitous list of nine data elements. “***This scan may include*** a detailed  
12 examination of all system files, designated application files, the registry, performance counters,  
13 hardware configuration, logs, running tasks, services, network connections, and other relevant data.  
14 The results of each scan are compressed and transmitted over network 106 in the form of a  
15 ‘snapshot’ to the Collector component 108.” ’936 Patent at 6:26-33. Nothing in this passage  
16 imposes a requirement that any particular data—much less all nine of them—must be included.

17 Rather, the emphasis is on flexibility and breadth, which the specification expressly  
18 contemplates: “the data collected can be voluminous. For example, in one embodiment, the data  
19 collected from a single machine, referred to as the ‘health check’ or snapshot for the machine,  
20 includes values for hundreds of thousands of attributes.” ’936 Patent at 21:65-22:5.

21 Similarly, the specification explains that creating a snapshot “involves collecting a massive  
22 amount of data and can take anywhere from a few minutes to hours to execute, depending on the  
23 configuration of the client.” *Id.* at 8:67-9:5. These passages make clear that a snapshot is not a  
24 static, arbitrary list of attributes, but a comprehensive and adaptable concept encompassing relevant  
25 data as needed. Fortinet’s reliance on the ’936 Patent at column 5 is misplaced. That passage  
26 describes data collected in a particular embodiment, not a universal requirement. *Id.* at 5:36-48.

Lacking meaningful intrinsic support, Fortinet resorts to three unrelated technical dictionaries—each offering a different definition, none of which matches Fortinet’s proposed construction. The only commonality among those definitions is that a snapshot includes data from a computer’s memory. None of the three dictionaries, individually or collectively, impose Fortinet’s rigid nine-element list.

Because both the intrinsic evidence and Fortinet’s own extrinsic evidence support the plain and ordinary meaning reflected in the claims, the Court should reject Fortinet’s construction and adopt the plain and ordinary meaning of “snapshot.”

## 2. “anomaly” (’936 Patent, claims 1, 2, 10, 12, 13, 18)

| Netskope’s Construction    | Fortinet’s Construction                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Plain and ordinary meaning | “an undesirable changes or an unexpectedly present asset, an unexpectedly absent asset, or an asset that has an unknown value” |

The primary examiner, the Board of Patent Appeals and Interferences (“PTAB”), intrinsic evidence, and even Fortinet’s own citations all confirm that “anomaly,” as used in the context of the ’936 Patent, should be construed according to its plain and ordinary meaning.

From the time the application that became the ’936 Patent was first filed, the term “anomaly” appeared within the independent claims. Ex. 6 at 3. Throughout prosecution, it was consistently described through scenarios where a system detected an unexpectedly present asset, an unexpectedly absent asset, or an asset with an unknown value. *See* Ex. 6. The primary examiner, who flagged minor infractions like the use of “comprises” in the Abstract, responded to the application six times and never questioned the meaning of “anomaly.” *See generally* Ex. 6.

The PTAB, reviewing the case on an unrelated prior art rejection, also accepted the plain and ordinary meaning, in that instance as explicitly defined by the specification: “[a]ppellant’s Specification discloses that ‘[a]n anomaly is defined as an unexpectedly present asset, an unexpectedly absent asset, or an asset that has an unknown value.’ Ex. 6 at 80. Fortinet’s proposed definition improperly includes “an undesirable changes [*sic*] or,” without any rational basis for expanding the term beyond its clear scope. Ex. 2 at 6.

Aside from citing the Decision on Appeal, which directly contradicts its own position, Fortinet relies on columns 7:60-8:29 of the specification as allegedly supporting its construction.

*Id.* The relevant portion of the cited specification states:

**An anomaly is defined as an unexpectedly present asset, an unexpectedly absent asset, or an asset that has an unknown value.** Anomalies are matched against a library of Recognition Filters 216. A Recognition Filter 216 comprises a particular pattern of anomalies that indicates the presence of a particular root cause condition or a generic class of conditions.

'936 Patent, 8:12-18

Fortinet's attempt to incorrectly insert additional limitations fails for at least two reasons. First, "anomaly" should be afforded its plain and ordinary meaning because the prosecution history and intrinsic evidence both show the term is readily understood by one of ordinary skill in the art. Second, even if construction were necessary, the term should be construed according to the language explicitly provided in the specification and adopted by the PTAB during prosecution. *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 862 (Fed. Cir. 2004) ("[T]he inventor's written description of the invention, for example, is relevant and controlling insofar as it provides clear lexicography"); also *AstraZeneca AB, Aktiebolaget Hassle, KBI-E, Inc. v. Mutual Pharmaceutical Co.*, 384 F.3d 1333, 1339 (Fed. Cir. 2004) (holding that using the term "defined below" indicated the patentee's clear intent of lexicography).

The intrinsic record, the PTAB's interpretation, and the absence of any other evidence from Fortinet confirms that Netskope's proposed construction is correct. Fortinet's attempt to inject extraneous limitations lacks support in the claims, specification, or prosecution history and should be rejected.

#### E. '153 Patent

##### 1. "arbitrary number of attributes" ('153 patent, claims 1, 10, and 15)

| Netskope's Construction    | Fortinet's Construction |
|----------------------------|-------------------------|
| Plain and ordinary meaning | Indefinite              |

Fortinet asks this Court to construe "arbitrary number of attributes" as indefinite even though the claim language, specification, and prosecution history all indicate that one of ordinary skill in the art would understand the plain and ordinary meaning.

1 For example, each user profile can have attributes attached to it. '153 Patent at 2:32-38.  
2 Upon joining the network, the control device can analyze the attributes for that profile to determine  
3 the bandwidth limitations and any traffic rules or conditions that may be associated with those  
4 attributes. *Id.* at 2:44-60. These attributes may vary depending on the user, with some profiles not  
5 having the same number of attributes depending on the needs of the system. "In some cases, the  
6 retrieved profile may not provide values for each of these attributes. Therefore, the control device  
7 can determine if the received user profile is complete, and, if it is not complete, can fill in the  
8 missing attribute values with default values." *Id.* at 5:34-43.

9 A POSITA, at the time of filing, would understand that the control device would assign a  
10 bandwidth limitation to multiple profiles, even if each profile had a different number of attributes  
11 assigned to it. *See* Ex. 4 at ¶ 87. Dr. Striegel also notes how this will not affect the performance of  
12 the system. "Because the number of missing attributes may vary from user to user, the number of  
13 attributes set to default values will also vary. Importantly, each user profile is assigned a traffic  
14 rule—regardless of how many attributes are defaulted. As a result, the number and type of attributes  
15 used to determine each user's bandwidth may differ, enabling flexible and individualized  
16 bandwidth management." *Id.* at ¶ 89. "As the traffic rules are still able to perform the communication  
17 relay and dynamically provision bandwidth to the users based on the traffic rules, the number of  
18 attributes is arbitrary." *Id.* at ¶ 90. The specification supports this understanding by explaining the  
19 variable number of attributes enables flexible system-wide bandwidth management while still  
20 allowing for granular modifications on the individual level. *See* '153 Patent at 7:22-37.

21 The prosecution history further confirms that a POSITA would not view the term as  
22 indefinite. The application, filed on July 20, 2009, underwent four years of rigorous examination,  
23 during which the examiner issued multiple rejections—including prior art rejections, double  
24 patenting rejections, and subject matter eligibility rejections under §101. In the course of this  
25 thorough review, the term "arbitrary number of attributes" was amended into the claim language in  
26 the November 18, 2013, Amendments and Response to Office Action. *See* Ex. 7. Following that  
27 amendment, and after four prior rounds of prosecution, the primary examiner issued a Notice of  
28

1 Allowance. At no point—including when the term was introduced—did the primary examiner raise  
 2 an indefiniteness rejection. Fortinet’s reliance on the prosecution history to support its  
 3 indefiniteness argument is therefore misplaced. To the contrary, the examiner’s detailed scrutiny  
 4 and ultimate allowance strongly supports that the claim language is clear and understood by a  
 5 POSITA.

6 Accordingly, because the record provides ample support for the plain and ordinary meaning  
 7 of “arbitrary number of attributes” and nothing indicates indefiniteness, the Court should adopt the  
 8 term’s plain and ordinary meaning.

9 **F. ’697 Patent**

10 **1. “generating an alert” (’697 Patent, claims 1, 15, 24)**

| Netskope’s Construction    | Fortinet’s Construction                   |
|----------------------------|-------------------------------------------|
| Plain and ordinary meaning | “a notification sent by a network sensor” |

12 As with the other terms that Fortinet disputes, “generating an alert” of the ’697 Patent  
 13 represents a simple collection of words that would be readily understood by a POSITA. In this case,  
 14 “generating an alert” describes an action performed by the claimed invention, and as described  
 15 more fully below, Netskope’s plain and ordinary meaning construction is clearly supported by the  
 16 claims, specification, and figures. Fortinet asks the Court to construe this term in a way that  
 17 expressly incorporates a device into the claimed action, and confusingly, in a way that turns an  
 18 action (“generating...”) into an object (“a notification...”). For these reasons, the Court should  
 19 adopt Netskope’s construction.

20 Starting with the claims, the term “generating an alert” appears in asserted claims 1, 15, and  
 21 24—none of which require that the alert be generated by a network sensor. For example, the  
 22 relevant portion of claim 1 reads:

23 A method of network based malware detection in a service provider  
 24 network, the method comprising:

25 ...

26 ***generating an alert*** identifying a network address associated with  
 the access device, the malware ID and the OS ID associated with  
 TCP session that generated the alert.

27 ’697 Patent at claim 1. Claims 15 and 24 mirror this same claim language. As shown above, the  
 28 claim limitation does not define *what* generates the alert. Indeed, neither the claims nor the

1 specification places a requirement on what component or device generates the alert that identifies  
 2 the network address. For example, the specification describes the generation of the alert as:

3 “If malware is present in the TCP session an associated malware ID  
 4 is determined by comparing a malware signature to the one or more  
 5 TCP packets, an alert identifying a network address associated with  
 6 the access device is generated with the malware ID and the OS ID  
 7 associated with TCP session that generated the alert.”

8 ’697 Patent at 2:7-18.

9 The ’697 Patent repeats similar passages in other portions of the specification—none of  
 10 which define or specify a component that generates the alert. *See* ’697 Patent at 3:28-36; 1:52-2:43,  
 11 3:48-4:9, 4:50-5:62, 7:38-9:43. Analyzing the ’697 Patent’s figures produces a similar result.  
 12 Indeed, none of the eight figures attached to the ’697 Patent demonstrate **how** or **what** mechanism  
 13 generates the alert. *See* generally ’697 Patent at Figs. 1, 3, 5-8. While the patent describes one  
 14 embodiment in which an alert **may** be generated by a network sensor, ’697 Patent at 4:60-63,  
 15 limitations from one embodiment should not be imported into the invention as a whole. *See*  
 16 *Decisioning.com, Inc. v. Federated Dep’t Stores, Inc.*, 527 F.3d 1300, 1314 (Fed. Cir. 2008) (“Th[e]  
 17 description of a preferred embodiment, in the absence of a clear intention to limit claim scope, is  
 18 an insufficient basis on which to narrow the claims.”); *Johnson Worldwide Assocs., Inc. v. Zebco*  
 19 *Corp.*, 175 F.3d 985, 992 (Fed. Cir. 1999) (“[J]ust as the preferred embodiment itself does not limit  
 20 claim terms ... inferences drawn from the description of an embodiment of the invention cannot  
 21 serve to limit claim terms ... as they are insufficient to require a narrower definition of a disputed  
 22 term.”)

23 Fortinet’s construction also improperly turns an action (“generating an alert”) into an object  
 24 (“a notification sent by a network sensor”). This alone renders the construction unworkable for  
 25 purposes of analyzing infringement and invalidity. For example, with Fortinet’s proposed  
 26 construction, claim 1 would recite:

27 ... the **method**...comprising:  
 28 receiving one or more transmission control protocol (TCP) packets...;  
 determining an operating system identifier...;  
 determining if malware is present...; and  
**a notification** sent by a network sensor....

1 It is not clear how infringement would be analyzed under Fortinet’s proposed construction. For  
 2 example, assuming that a Fortinet product performs the “receiving,” and two “determining” steps,  
 3 would the product infringe as long as the notification *exists*, or is something more required? Fortinet  
 4 effectively proposes a new type of claim format—the method-plus-data format—for which there is  
 5 no legal precedent for how the claim should be treated for purposes of infringement and invalidity.

6 Further, none of the intrinsic evidence cited by Fortinet supports its construction. While  
 7 Fortinet cites to claims 3, 12, and 13 of the ’697 Patent, Ex. 2 at 10, these claims describe the system  
 8 sending a notification to the subscriber account associated with the access device, along with  
 9 summarizing the information within the alerts. None of these claims describe *how* or by *what*  
 10 mechanism the alert is generated, nor do they advance Fortinet’s proposed construction that the  
 11 alert must be generated by a network sensor. As another example, the passage in column 4 relied  
 12 on by Fortinet does not support Fortinet’s construction. ’697 Patent at 4:29-41. This passage recites  
 13 the same information used to support Netskope’s plain and ordinary meaning construction—that  
 14 the system “can provide a notification to the subscriber that a computer running a specific operating  
 15 system is infected and direct them to remedy that infection.” ’697 Patent at 4:37-41. As another  
 16 example, Fortinet cites to the specification at 5:63-6:13, which describes the *multiple* ways in which  
 17 subscribers receive notifications.

18 As shown by Fortinet’s own evidence, the recited alert may be generated by multiple  
 19 mechanisms, and Fortinet has provided no basis for (i) turning the action into an object, and (ii)  
 20 requiring that the network sensor must generate the alert. Accordingly, the Court should reject  
 21 Fortinet’s unfounded construction.

## 22 2. “service provider network” (’697 Patent, claims 1, 15, 24)

| Netskope’s Construction    | Fortinet’s Construction             |
|----------------------------|-------------------------------------|
| Plain and ordinary meaning | “internet service provider network” |

25 The term “service provider network” should be construed according to its plain and ordinary  
 26 meaning because Fortinet’s proposed construction adds an unnecessary qualifier that contradicts  
 27 the specification and improperly narrows the claim language.

1 This claim term already consists of common words with clear meanings: a network operated  
2 for a service provider. By contrast, an “internet service provider network” (“ISP”) is a term of art  
3 referring to the network from “a business that supplies Internet connectivity services to individuals,  
4 businesses and other organizations.” Ex. 1 at 284, 291. In other words, while the plain and ordinary  
5 meaning of this claim term covers any network operated by a service provider, Fortinet’s proposed  
6 construction would limit it to a network operated by AT&T, Comcast, and other businesses that  
7 provide Internet connectivity services. This drastically narrows the claim in a way not contemplated  
8 by the claim or the specification. Fortinet’s attempt to inject a term of art, where the patentee  
9 deliberately chose not to use one, should be rejected.

10 This deliberate choice to not limit the claims to an ISP is confirmed by the specification.  
11 Figure 1 shows the service provider network 110 as separate and distinct from the internet at 120.  
12 The accompanying text reinforces this distinction: “TCP/IP traffic is received at the network edge  
13 node 112 which routes the data through the SP network 110 to the Internet 120.” ’697 Patent at  
14 4:22-25. The only time the specification mentions an internet service provider network, it does so  
15 disjunctively, presenting it as an alternative to the service provider network: “FIG. 1 depicts, in a  
16 block diagram, a system for operating system identification and malware remediation. A user  
17 location 100 comprises multiple computing devices 104, 106, 108 in a local area network (LAN)  
18 that access an Internet service provider or service provider (SP) network 110 via an access device  
19 102.” ’697 Patent at 4:11-16. Thus, the specification indicated that a device in a LAN could connect  
20 to an ISP network or an SP network, denoted as 110. Given the greater breadth of a “service  
21 provider,” compared to the limited set of business that are ISPs, it is unsurprising that the claims  
22 recited a *service provider network* and not an *ISP* network. The claim language reflects a deliberate  
23 choice between two options—not an ambiguity to be “remedied” by rewriting the term.

24 Fortinet’s reliance on prosecution history does not change this analysis. Specifically, during  
25 prosecution the applicant remarked that “[o]ne or more embodiments of the claimed invention  
26 provide a system and method that allows network based malware detection to be used effectively  
27 in a service provider's network, where the devices are typically connected to the network through  
28

an access device, such as a modem or router.” Ex. 8 at 9. The remarks explained the novelty of the invention in the context of a service provider’s network, where devices connect through an access device such as a modem or router. This is consistent with the specification, which depicts devices 104, 106, and 108 connected to router 102, which in turn connects to the service provider network 110—distinct from the Internet 120. The specification confirms this: “[t]he system of the present disclosure, or parts thereof as described further below, are deployed within the SP network in order to capture and analyze the network traffic. Using the analyzed traffic, the system can determine if a subscriber's computer 104 is infected with malware.” ’697 Patent at 4:33-36.

In sum, the claim language, specification, and prosecution history all confirm that “service provider network” was deliberately chosen and is distinct from “internet service provider.” Fortinet’s construction improperly injects a term of art that the patentee intentionally avoided. The Court should therefore adopt the plain and ordinary meaning of “service provider network.”

Dated: January 5, 2026

**PERKINS COIE LLP**

By: /s/ Kyle R. Canavera

Thomas N. Millikan, Bar No. 234430  
Joseph P. Reid, Bar No. 211082  
Kyle R. Canavera, Bar No. 314664  
Andrew N. Klein, Bar No. 300221  
Hessam Gharaviram, Bar No. 345690  
Ashlee E. Sherman, Bar No. 348085  
Sarah M. Anderson, Bar No. 359690

*Attorneys for Plaintiff Netskope, Inc.*